DeTeWe

Your connection to the world

OpenComNet 20

Bedienungsanleitung

Willkommen bei DeTeWe

Vielen Dank, dass Sie sich für ein Produkt von DeTeWe entschieden haben. Unser Produkt steht für höchste Qualitätsansprüche, gepaart mit hochwertigem Design.

Die folgende Bedienungsanleitung wird Sie beim Gebrauch Ihres Routers OpenComNet 20 begleiten und dabei alle wesentlichen Fragen beantworten.

Sollten Sie darüber hinaus Informationen benötigen, stehen Ihnen unter

www.detewe.de

auf den Supportseiten die aktuellsten Hinweise und Informationen zur Verfügung.

Wir wünschen Ihnen viel Freude mit Ihrem Router OpenComNet 20.

Inhaltsverzeichnis

Umgang mit dem OpenComNet 20 1

Sicherheitshinweise 1
Bestimmungsgemäße Verwendung / Konformitätserklärung 1
Grundsätzliches 1
Stromversorgung 1
Aufstellungsort 2
Überblick und Basiswissen 3
Allgemeines 3
Ihr ISDN-Anschluss 3
ADSL 4
Anschlüsse 4
Bedeutung der Leuchtdioden 5
Software-Ausstattung 6

Installation 7

Voraussetzungen für den Betrieb 7
Was wurde geliefert? 7
Anforderungen an die PCs 7
Reihenfolge der Installation 8
Details zur Montage 9
Montageort 9
Tischaufstellung 10
Wandmontage 10
Anschluss der PCs 10
PC Konfiguration 11
Windows Clients 11
TCP/IP Einstellungen - Übersicht 11
Überprüfen der TCP/IP Einstellungen unter Windows 98 SE 12
DHCP benutzen 12
Überprüfen der TCP/IP Einstellungen unter Windows 2000 13
DHCP benutzen 13
Feste IP-Adresse benutzen (Checkbox: Folgende IP-Adresse verwenden) 14
Überprüfen der TCP/IP Einstellung unter Windows XP 14
Feste IP-Adresse benutzen (Checkbox: Folgende Adresse verwenden) 15
Internetzugang 16
Windows 98 SE/2000 16
Windows XP 16
Macintosh Clients 17
- Mac OS 17
- Mac OS X 18
Linux Clients 20
Andere auf Unix basierende Betriebssysteme 20

Konfiguration des OpenComNet 20 21
Werkseinstellungen 22
Der Assistent 23
Vorbereitungen 23
So benutzen Sie Ihren Browser 23
Navigieren im Menü und Dateneingabe 25
Assistent 26
Der Konfigurator 30
Internet 31
DSL 32
ISDN-Fallback 33
Dynamisches DNS 35
System 37
Passwort 38
Fernwartung 39
Fernzugriff 40
Datensicherung 41
- Konfiguration sichern 41
- Konfiguration wiederherstellen 42
Firmware Update 43
Neustart 44
Uhr 45
- Uhr manuell setzen 46
- SNTP 47
Konten 49
DSL 50
ISDN Fallback 51
LAN 52
IP-Adresse 53
DHCP Server 55
DNS 59
Routen 64
NAT 67
- IP-Adressen 68
- Virtueller Server 69
- Spezielle Anwendungen 74
Sicherheit 76
Allgemein 77
Firewall 79
- Zugangskontrolle 80
- Filtern von Paketen 82
Hacker-Abwehr 84

Besondere Leistungsmerkmale 86
System-Info 87
Installation des Druckertreibers für den Netzwerkdrucker 90
Windows 2000 90
Windows XP 90
Windows 98 SE 91
Mac OS X 92
Software installieren 93
Informationen über die Software 93
Starten des Installationsprogramms 93

Konfiguration Telefonanwendung 94
PC Voraussetzungen 94
Installation der Software 94
Der Installationsassistent 95
CAPIControl Einstellungen 96
HomeNet Control Einstellungen 101

Kommunikationssoftware installieren 103
Konfigurationsassistent WinSuite 103

Anhang 110
Technische Daten 110
Pflege und Wartung 111
Umwelteigenschaften und Entsorgung 111
Port Forwarding Regeln 112
Glossar 116
Service und Gewährleistung 123
Konformitätserklärung 124
Stichwortverzeichnis 125
Notizen 127
Bohrschablone 128

Umgang mit dem OpenComNet 20

Sicherheitshinweise

Bestimmungsgemäße Verwendung / Konformitätserklärung

Dieses Produkt kann in allen EU-Mitgliedsstaaten an einem ISDN-Basisanschluss, der das EURO-ISDN-Protokoll DSS1 unterstützt, betrieben werden.
Das CE-Zeichen auf dem Produkt bestätigt seine Konformität zu den technischen Richtlinien zur Benutzersicherheit und elektromagnetischen Verträglichkeit, gültig zum Zeitpunkt der Ausstellung der entsprechenden Konformitätserklärung nach europäischer Direktive 99/5/EC.
Die Konformitätserklärung ist unter http://www.detewe.de im Internet einzusehen.
Bitte benutzen Sie auch die anderen Dokumentationen, die zu den Teilen Ihres Routers mitgeliefert wurden.

Grundsätzliches

Das Gehäuse darf nicht geöffnet werden. Durch unbefugtes Öffnen des Gehäuses und unsachgemäße Reparaturen können Gefahren für die Benutzer entstehen und der Garantieanspruch erlischt.

Defekte Stecker oder Steckernetzgeräte mit defektem Gehäuse dürfen nicht weiter benutzt werden, es besteht die Gefahr eines elektrischen Schlages. Lassen Sie diese Teile umgehend gegen Original-Ersatzteile austauschen.

Lassen Sie keine Flüssigkeit in das Innere des OpenComNet 20 eindringen, da sonst elektrische Schläge oder Kurzschlüsse die Folge sein könnten.

Während eines Gewitters dürfen Sie den OpenComNet 20 nicht installieren und auch keine Leitungsverbindungen stecken oder lösen.

Der OpenComNet 20 ist nur für Anwendungen innerhalb eines Gebäudes vorgesehen. Verlegen Sie die Leitungen so, dass niemand darauf treten oder darüber stolpern kann.

Stromversorgung

Dieses Produkt benötigt eine 230-V-Wechselstromversorgung. Der Strom ist bei diesem Produkt nur abzuschalten, indem das Netzteil aus der Steckdose gezogen wird.

Aufstellungsort

Legen Sie den OpenComNet 20 auf eine flache, ebene Oberfläche oder montieren Sie ihn an der Wand. Vermeiden Sie bei der Aufstellung die direkte Nähe von:

- Wasser, Feuchtigkeit oder feuchten Orten (z. B. Bad)
- Hitzequellen, direkter Sonneneinstrahlung oder ungelüfteten Orten
- Geräten, die starke, magnetische Felder erzeugen, Elektrogeräten, Leuchtstofflampen, Computern, Radiogeräten, Fernsehern oder Telefax- und Telefongeräten
- Orten, an denen das Gerät verdeckt werden kann, seine Lüftung behindert wird, Flüssigkeit hinein gelangen kann
- staubigen Orten, und Orten, die Schwingungen, Erschütterungen oder extremen Temperaturschwankungen ausgesetzt sind.

Achten Sie darauf, dass sich das Gerät nicht im Zugriffsbereich kleiner Kinder befindet.

Ihr Gerät wird für normale Gebrauchsbedingungen gefertigt. Die heutigen Möbel sind mit einer unübersehbaren Vielfalt von Lacken und Kunststoffen beschichtet und werden mit unterschiedlichen Lackpflegemitteln behandelt. Es ist nicht auszuschließen, dass manche dieser Stoffe Bestandteile enthalten, die die Kunststofffüße des Gerätes angreifen und erweichen. Die so durch Fremdstoffe veränderten Gerätefüße können auf der Oberfläche der Möbel unliebsame Spuren hinterlassen.
Der Hersteller kann aus verständlichen Gründen für derartige Schäden nicht haften. Verwenden Sie daher - besonders bei neuen oder mit Lackpflegemitteln aufgefrischten Möbeln - für Ihr Gerät bitte eine rutschfeste Unterlage.

Hinweis

- Bitte achten Sie darauf, das Gerät nicht im Öffnungsbereich von Türen oder Fenstern zu montieren: Gefahr der Beschädigung !

Überblick und Basiswissen

Allgemeines

Der OpenComNet 20 ist ein Router mit eingebautem DSL-Modem, der Ihnen eine Vielzahl von Anschluss- und Konfigurationsmöglichkeiten bietet:

- Einen Anschluss an das ISDN (Mehrgeräteanschluss).
- Einen Anschluss für DSL (UR2-Anschluss zum Splitter).
- Einen Anschluss für einen zentralen Netzwerkdrucker.
- Vier LAN-Ports (10/100 MBit/s) zum Errichten eines lokalen Netzwerkes.

Der integrierte Router ermöglicht es allen angeschlossenen PCs, gleichzeitig eine aktive Internet-Verbindung zu haben (Time Sharing-Verfahren). Zum Aufbau einer Internetverbindung genügt z. B. der Start eines Browsers (z. B. Microsoft Internet Explorer oder Netscape Communicator). Die automatische Überwachung sorgt dafür, dass nach einer einstellbaren Zeit ohne Datenverkehr (z. B. nach 3 Minuten) die Verbindung getrennt wird.

Mit der beigefügten Software WinSuite können Sie mit Ihren PCs über eine LAN-Schnittstelle Anwendungen FAX-, SMS-, MMS-Center, PC-Telefonie, Wahlhilfe, Anrufbeantworter, Eurofiletransfer, Adressbuch und Journal nutzen.

Ihr ISDN-Anschluss

Das ISDN ist ein Kommunikationsnetz in digitaler Technik. Es integriert gleichzeitig die Übertragung von Sprache (Telefonnetz) und Daten (Telefax, Telex, Datex), daher der Name Integrated Services Digital Network (diensteintegrierendes digitales Netz). Der Anschluss ist europaweit genormt und wird als Euro-ISDN-Anschluss bezeichnet.
Ihr Router OpenComNet 20 ist für den Anschluss an einen Euro-ISDN-Mehrgeräteanschluss bestimmt. Er funktioniert nicht am Euro-ISDN-Anlagenanschluss oder an einem Anschluss mit einem anderen Protokoll als DSS1.

Hinweis: An einem ISDN-Anschluss können Sie bis zu acht ISDN-Geräte betreiben. Wenn Sie neben Ihrem OpenComNet 20 weitere ISDN-Geräte anschließen wollen, erkundigen Sie sich bitte bei Ihrem Fachhändler.

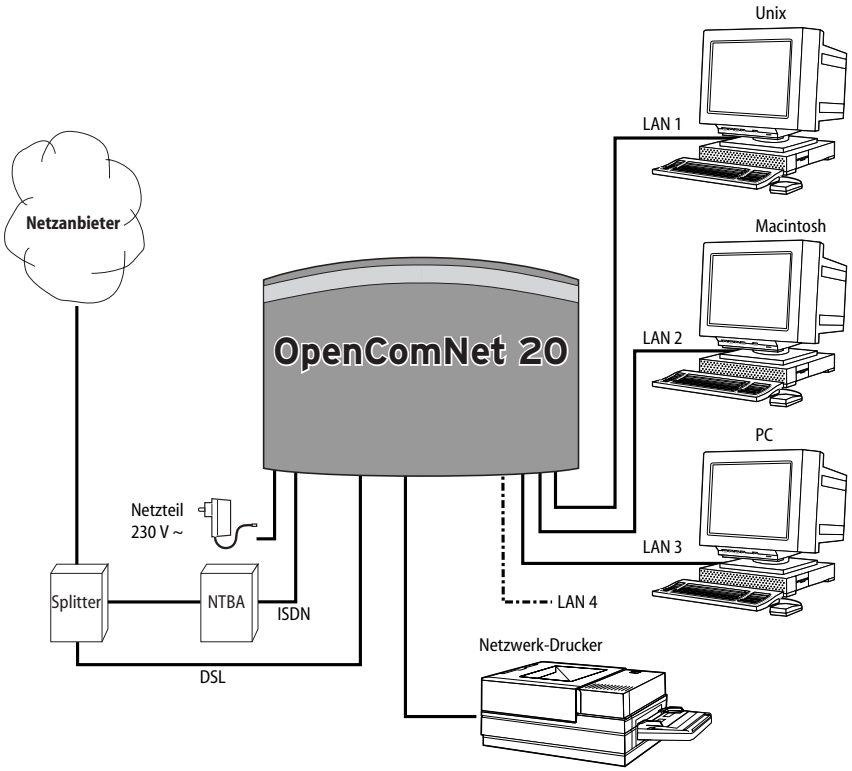
ADSL

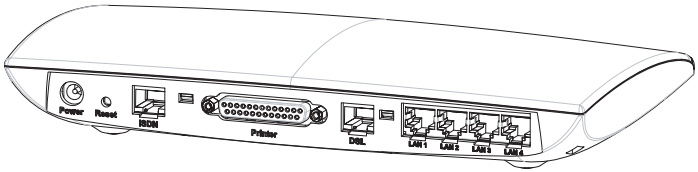
An einem ADSL-Anschluss sind Datenübertragungsraten von Ihrem PC zum Internet (Upload) von 128 kBit/s und vom Internet zu Ihrem PC (Download) von 768 kBit/s möglich.

Je nach Anschlusstyp/- tarif sind auch erheblich höhere Datenraten möglich. Diese werden ebenfalls von Ihrem OpenComNet 20 unterstützt.

Das notwendige Zusatzgerät (Splitter (BBAE)) erhalten Sie zusammen mit dem entsprechenden Anschlusskabel und weiteren Informationen bei Ihrem Netzbetreiber.
Ein DSL-Modem ist bereits im OpenComNet 20 eingebaut.

Anschlüsse



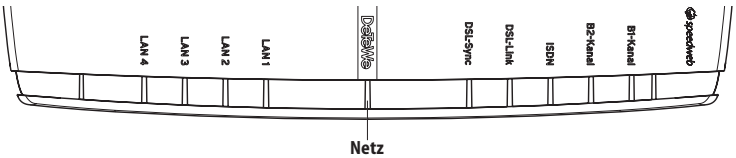


- **Power**: Schließen Sie hier das Steckernetzteil an.
- **RESET**: Diese Taste veranlasst den Neustart des Routers, Sie haben zwei Möglichkeiten:
  - Taste kurz gedrückt führte einen Neustart aus
  - Taste länger als 20 Sekunden gedrückt setzt das Gerät in den Auslieferungszustand zurück. Lassen Sie dann die Taste los und warten Sie bis die Werkseinstellungen geladen sind.
- **ISDN**: Verbinden Sie diesen Anschluss mit dem NTBA.
- **Printer**: Schließen Sie hier einen Netzwerk-Drucker an (Länge des Kabels < 3m).
- **DSL**: Verbinden Sie diesen Anschluss mit dem Splitter Ihres Netzbetreibers.
- **LAN 1**…**4** Schließen Sie hier Ihre PCs an. Verwenden Sie dazu Standard-Cat. 5 - Netzwerkkabel (nur geschirmte Ausführung verwenden) mit RJ45 Steckern. Sie können Crossover- und Parallel-Kabel gleichermaßen einsetzen.

Hinweis

Jeder LAN Anschluss (LAN) kann zur Erweiterung des Netzwerkes verwendet werden. Dieses wird automatisch als „UPLINK" erkannt. Die Zusammenschaltung erfolgt mit Standard-Cat. 5 - Netzwerk-kabeln.

Bedeutung der Leuchtdioden



Die Leuchtdioden an der Oberseite des OpenComNet 20 haben folgende Bedeutung:

- **B1-Kanal** bzw. **B2-Kanal** leuchtet: Der entsprechende B-Kanal ist belegt. Blinkt bei Datentransfer.
- **ISDN** leuchtet: … wenn das ISDN-Kabel richtig installiert wurde.
- **DSL-Link** leuchtet: … wenn eine Verbindung zum Internet besteht. Blinkt wenn Datentransfer.
- **DSL-Sync** leuchtet: … wenn sich das DSL-Modem synchonisiert hat, blinkt während der Synchonisationsphase.
- **LAN 1**…**4** leuchtet: Es besteht eine Verbindung zum angeschlossenen PC.
  LAN 1…**4** blinkt: Zwischen dem Router und dem angeschlossenen PC werden Daten übertragen.
- **(Netz)** leuchtet, wenn die Stromversorgung vorhanden ist.

Software-Ausstattung

- **DSL Routing**
- **ISDN Routing**
- **ISDN Fallback**
  automatische Umschaltung auf ISDN bei DSL-Ausfall einrichtbar.
- **DNS Relay und Server** (Domain Name Server)
  ermöglicht die automatische Umsetzung von Namen in IP-Adressen.
- **DHCP Server** (Dynamic Host Configuration Protocol)
  weist IP-Adressen im LAN automatisch zu.
- **NAT / PAT** (Network / Port Adress Translation)
  für die Nutzung privater IP-Adressen, die im Internet ungültig sind. So wird verhindert, dass von außen unerwünschte Verbindungen zu einzelnen Arbeitsplätzen hergestellt werden können.
- **Firewall-Funktionen** über vorkonfigurierte Sicherheitsstufen und/oder individuelle Filter einrichten. Angriffschutz gegen DoS-Attacke (Denial of Service).
- **Port Forwarding** um auch Server-Applikationen, Online-Spiele, Tauschbörsen usw. zu unterstützen, können Portbereiche definiert werden, deren Traffic direkt auf spezielle PCs im lokalen Netzwerk geleitet wird.
- **Volumen- und Zeitkonten** zur Gebührenkontrolle.
- **Internetsperre** mit Passwortschutz.
- **LAN-CAPI-Funktion für 10 PCs** zur Unterstützung von ISDN-Anwendungen.
- **CAPI Control** (Common-ISDN-Application Interface)
  gewährleistet die Überwachung und Einstellung von ISDN-Merkmalen.
- **HomeNet Control** ermöglicht die Überwachung der Router-Funktionen.
- **Sex Dialer Sperre** Sperreinrichtung zum Schutz vor „Abzockernummern".
- **Web-Konfigurator** ermöglicht die benutzerfreundliche Einrichtung des Routers.
- **Kommunikationssoftware WinSuite** mit FAX-, SMS-, MMS-Center, PC-Telefonie, Wahlhilfe, Anrufbeantworter, Eurofiletransfer, Adressbuch und Journal
- **Fernwartung** über die DeTeWe-Hotline oder DeTeWe-Vertragshändler möglich.
- **Fernzugriff** Möglichkeit des Zugriffs auf den Router von außerhalb über ISDN für den Betreiber des Routers.
- **Dynamisches DNS** Umsetzung der dynamischen IP-Adresse auf einen festen Domain-Namen, um Zugriff aus dem Internet zu ermöglichen.

Installation

Voraussetzungen für den Betrieb

Was wurde geliefert?

Überprüfen Sie den Inhalt der Verpackung auf Vollständigkeit:
1 ADSL-/ISDN-Router OpenComNet 20
1 Steckernetzteil,
1 ISDN-Anschlusskabel,
1 DSL-Anschlusskabel,
1 CD-ROM mit Installationssoftware für Windows 98 SE/2000/ XP
1 Benutzerhandbuch für OpenComNet 20 (dieses Dokument)
1 Kurzanleitung - Der schnelle Weg zum Ziel

Auf der CD-ROM befinden sich folgende Komponenten:
- Firmware mit UPnP
- Firmware ohne UPnP
- Das Setup der Treibersoftware mit Common ISDN Application Programming Interface (CAPI) sowie CAPI Port, CAPI Control und TAPI-Treiber.
- Die Kommunikationssoftware WinSuite für Windows 98 SE/2000/XP mit FAX-, SMS-, MMS-Center, PC-Telefonie, Wahlhilfe, Anrufbeantworter, Eurofiletransfer, Adressbuch und Journal.
- Die ausführliche Bedienungsanleitung für WinSuite.
- Diese Bedienungsanleitung und die Kurzanleitung als Online-Dokumente.
- Acrobat Reader.

Anforderungen an die PCs

Für die Installation der Konfigurationssoftware und WinSuite sind folgende Systemvoraussetzungen erforderlich:
- IBM-kompatibler PC mit Festplatte und CD-ROM-Laufwerk
- Taktfrequenz von 266 MHz oder höher
- Arbeitsspeicher mindestens 256 MB
- Microsoft Windows 98 SE/Me/2000/XP
- freie Festplattenkapazität von min. 20 MByte
- Für AB-Nutzung: Vollduplex Soundkarte (mit Mikrofon)
- Folgende Web Browser werden unterstützt:
  Internet Explorer ab Vers. 6.0
  Netscape ab Vers. 7.0
  Opera ab Vers. 7.0
  Mozilla ab Vers. 1.4
  Safari 1.2

- Ein Ethernet 10BaseT oder 100BaseTX-Anschluss (Netzwerkkarte)
- Außerdem muss der OpenComNet 20 bereits nach dem Anschlussschema installiert sein, wie im Kapitel „Anschlüsse“ beschrieben.

Bitte beachten Sie, dass Ihre Rechner zum Anschluss an eine LAN-Schnittstelle des OpenComNet 20 über eine Netzwerkkarte verfügen müssen. Sollte dies nicht der Fall sein, installieren Sie eine Netzwerkkarte entsprechend der Vorgaben des Herstellers. Die LAN-Schnittstellen des OpenComNet 20 verfügen über eine Datenübertragungsgeschwindigkeit von10/100 MBit/s.

Auf allen Rechnern im LAN muss das TCP/IP Protokoll installiert sein.

Wichtig:
Bevor Sie die Treibersoftware für den OpenComNet 20 installieren, muss eine eventuell bereits vorhandene ISDN-Karte ausgebaut sowie eventuell vorhandene CAPI-Treiber deinstalliert werden.

Reihenfolge der Installation

1. Montieren und verkabeln Sie den OpenComNet 20 wie es im Kapitel „Details zur Montage“ beschrieben ist.

2. Konfigurieren Sie Ihre Rechner wie im Kapitel „PC-Konfiguration“ beschrieben.

3. Fahren Sie alle Rechner herunter und schaltet Sie sie aus.

4. Schalten Sie erst Ihren OpenComNet 20 und **danach** alle angeschlossenen Rechner ein.

5. Konfigurieren Sie den OpenComNet 20.

6. Installieren Sie die Software auf Ihren PCs (siehe Seite 94).

Details zur Montage

Montageort

Die Umgebungstemperatur zum Betrieb des OpenComNet 20 darf +5 °C nicht unterschreiten und +40 °C nicht überschreiten. Montieren Sie daher den OpenComNet 20:

- nicht über oder vor Wärmequellen (z. B. Heizkörper),
- nicht an Stellen mit direkter Sonneneinstrahlung,
- nicht hinter Vorhängen,
- nicht in kleinen, unbelüfteten, feuchten Räumen,
- nicht im Freien und
- nicht auf oder in der Nähe von leicht entzündlichen Materialien.

Achten Sie weiterhin darauf,

- dass der Raum möglichst staubfrei und trocken ist;
- dass keine Hochfrequenzgeräte (z. B. Sender, Bestrahlungsgeräte oder ähnliche Geräte) in der Nähe stehen;
- dass unter keinen Umständen Flüssigkeiten herab tropfen und durch die Öffnungen in das Gerät gelangen können;
- dass die Wand für die Montage eben und tragfähig ist.

Für die Wahl des Montageortes sollten Sie folgende Kriterien berücksichtigen:

- Eine freie Steckdose für das Steckernetzteil in unmittelbarer Nähe.
- Richten Sie sich beim Aufstellen der Geräte nach den Längen der beiliegenden Kabel. Bei einer Ethernet-Verkabelung mit einem Cat.5 -Kabel beträgt die maximale Länge 100 m.

Die Steckdose zum Anschluss an das 230 V~-Netz muss von einer konzessionierten Elektrofachkraft installiert worden sein, um Gefahren für Personen und Sachen auszuschließen. Sorgen Sie jederzeit für freien Zugang zur Steckdose.

Sehen Sie einen separaten Stromkreis für den 230 V~-Anschluss des OpenComNet 20 vor. Dann setzen eventuelle Kurzschlüsse anderer Geräte der Haustechnik den OpenComNet 20 nicht außer Betrieb. Zum Schutz gegen Überspannungen, wie sie bei Gewittern auftreten können, empfiehlt sich die Installation eines Überspannungsschutzes. Lassen Sie sich von Ihrem Elektroinstallateur oder Ihrem Netzbetreiber beraten.

Tischaufstellung

Sie können den OpenComNet 20 einfach auf eine feste Unterlage legen, beispielsweise einen Tisch. Beachten Sie bitte, dass die Gummifüße des Gerätes unter Umständen Spuren auf der Möbeloberfläche hinterlassen können.

Wandmontage

Empfohlen werden:
- Rundkopf-Schrauben 4 x 30 mm (Holzschrauben)
- passende Dübel (6mm)

Weiterhin benötigen Sie folgendes Werkzeug:
- Bohrer 6 mm für Stein (entsprechend der gewählten Dübel, Bohrertyp hängt vom Material ab)
- Bohrmaschine (mit Schlag- oder Hammerwerk)
- Schraubendreher (passend zu den gewählten Schrauben)

Achtung! Vergewissern Sie sich, dass im Bereich der geplanten Bohrlöcher keine Versorgungsleitungen, Kabel oder ähnliches verlegt sind.

Bohren Sie die Löcher für die beiden Befestigungsschrauben im Abstand von 140 mm (s. Bohrschablone im Anhang).

Setzen Sie den Dübel ein und drehen Sie die Schrauben so tief in die Wand, dass zwischen Schraubenkopf und Wand noch ein Abstand von 4 mm verbleibt.

Hängen Sie dann das Gerät mit der Rückseite in die Schrauben ein und ziehen Sie sie etwas nach unten.

Anschluss der PCs

Schließen Sie nun die Rechner an den OpenComNet 20 an.

PC Konfiguration

Sie finden in diesem Kapitel alle Informationen, die für Ihr Netzwerk LAN nötig sind.

Die Konfiguration eines jeden PCs im Netzwerk muss überprüft und gegebenenfalls angepasst werden.

- TCP/IP Netzwerkeinstellungen
- Konfiguration des Internetzugangs
- Installation des Druckertreibers für den Netzwerkdrucker

Windows Clients

Sie erfahren hier wie ein Windows Client für den Internetzugang über den OpenComNet 20 konfiguriert sein muss.

Der erste Schritt ist die Überprüfung der TCP/IP Einstellungen.

Der OpenComNet 20 benutzt das TCP/IP Netzwerkprotokoll für alle Funktionen, daher ist es unbedingt erforderlich, dass das TCP/IP Netzwerkprotokoll auf jedem PC installiert und gleichartig konfiguriert ist.

TCP/IP Einstellungen - Übersicht

Wenn Sie die Standardeinstellungen vom OpenComNet 20 und die Standardeinstellungen von Windows TCP/IP noch nicht verändert haben, brauchen Sie weiter nichts zu tun.

- Standardmäßig wird der OpenComNet 20 als DHCP-Server arbeiten und automatisch eine korrekte IP-Adresse an jeden PC im Netzwerk senden, sobald dieser den Bootvorgang beendet hat.
- Bei allen nicht netzwerkfähigen Windows Versionen ist die TCP/IP Einstellung so, dass der PC als DHCP-Client arbeitet.

Verwenden Sie aber feste IP-Adressen auf einem PC, sind die folgenden Anpassungen erforderlich:

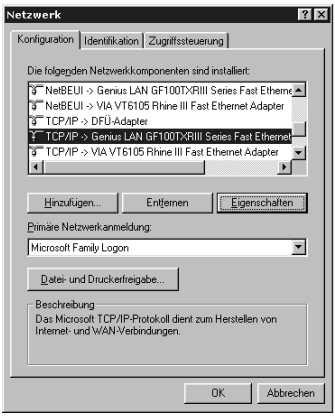
- Das „Gateway“ muss auf die IP-Adresse vom OpenComNet 20 eingestellt werden.
- Der DNS sollte auf die Adresse, die Ihnen Ihr Internetprovider gegeben hat, eingestellt sein.

Hinweis

Hat das bestehende Netzwerk bereits einen Standard-Router, muss der Systemadministrator diesen Router neu konfigurieren, siehe auch unter Kapitel „Besondere Leistungsmerkmale“.

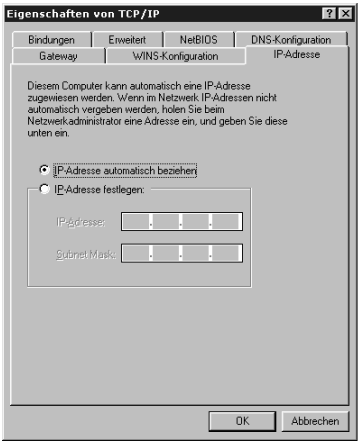
Überprüfen der TCP/IP Einstellungen unter Windows 98 SE

- Wählen Sie unter Systemeinstellungen den Punkt **Netzwerk** aus:



- Wählen Sie aus der Liste **TCP/IP** als Protokoll für Ihre Netzwerkkarte aus.

- Klicken Sie auf **Eigenschaften**.



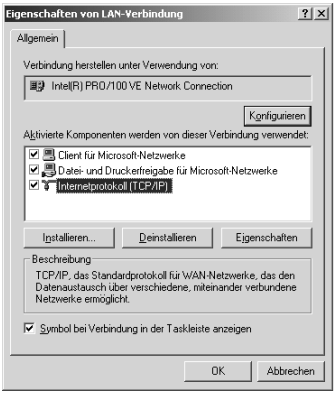
Stellen Sie sicher, dass die Einstellungen so sind wie nachfolgend beschrieben:

DHCP benutzen

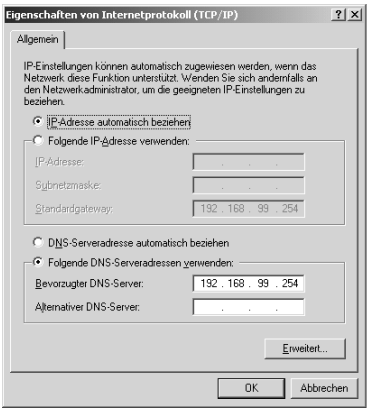
Um DHCP zu nutzen, wählen Sie **Eine IP-Adresse automatisch beziehen**. Dies ist die Standardeinstellung und wird empfohlen. Der OpenComNet 20 kann so als DHCP-Server arbeiten. Starten Sie den PC neu, um sicher zu gehen, dass der PC seine IP-Adresse neu vom OpenComNet 20 bekommt.

Überprüfen der TCP/IP Einstellungen unter Windows 2000

- Wählen Sie unter Start >Einstellungen >Systemsteuerung den Punkt **Netzwerk- und DFÜ-Verbindung**:
- Klicken Sie auf das Icon für **LAN-Verbindung** und dann auf **Eigenschaften**, Sie sehen das nachfolgende Fenster:



- Wählen Sie **TCP/IP Protokoll** für Ihre Netzwerkkarte aus.
- Klicken Sie dann auf **Eigenschaften**.



- Stellen Sie sicher, dass ihre Einstellungen so sind wie nachfolgend beschrieben.

DHCP benutzen

Aktivieren Sie den Knopf **Eine IP-Adresse automatisch beziehen**. Dies ist die Standardeinstellung von Windows und wird empfohlen. Der OpenComNet 20 kann so als DHCP-Server arbeiten.

Starten Sie den PC neu, um sicher zu gehen, dass der PC seine IP-Adresse neu vom OpenComNet 20 zugeteilt bekommt.

Feste IP-Adresse benutzen (Checkbox: Folgende IP-Adresse verwenden)

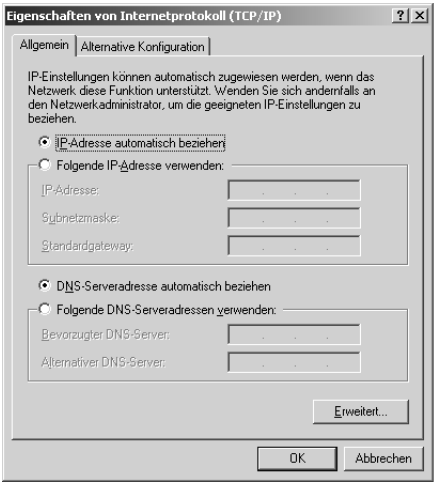
Ist Ihr PC bereits für ein Netzwerk konfiguriert, prüfen Sie zusammen mit dem Systemadministrator die Einstellungen und nehmen Sie nur dann Änderungen vor:

- Tragen Sie die IP-Adresse vom OpenComNet 20 ins Feld **Standard-Gateway** ein und klicken Sie auf **OK** (Ihr Systemadministrator kann Sie dabei unterstützen, dass Sie die richtige IP-Adresse zuweisen).
- Ist das Feld **Bevorzugter DNS Server** noch leer, wählen Sie die Checkbox **Folgende DNS-Serveradressen verwenden** und tragen Sie die IP-Adresse Ihres OpenComNet 20 (im Auslieferungszustand 192.168.1.1) ein. Klicken Sie dann auf **OK**.

Überprüfen der TCP/IP Einstellung unter Windows XP

- Wählen Sie unter Systemeinstellungen den Punkt **Netzwerkverbindungen**.
- Klicken Sie auf das Icon **LAN Verbindung** und dann auf **Eigenschaften**. Folgendes Fenster erscheint:

- Wählen Sie **TCP/IP Protokoll** für Ihre Netzwerkkarte aus.
- Klicken Sie dann auf **Eigenschaften**.



DHCP benutzen

Aktivieren Sie die Checkbox **IP-Adresse automatisch beziehen**. Dies ist die Standardeinstellung von Windows und wird empfohlen. Der OpenComNet 20 kann so als DHCP-Server arbeiten.
Starten Sie den PC neu, um sicher zu gehen, dass der PC seine IP-Adresse neu vom OpenComNet 20 zugeteilt bekommt.

Feste IP-Adresse benutzen (Checkbox: Folgende Adresse verwenden)

Ist Ihr PC bereits für ein Netzwerk konfiguriert, prüfen Sie zusammen mit dem Systemadministrator die Einstellungen und nehmen Sie nur dann Änderungen vor:

- Tragen Sie die IP-Adresse vom OpenComNet 20 ins Feld **Standard-Gateway** ein und Klicken Sie auf **OK** (Ihr Systemadministrator kann Sie dabei unterstützen, dass Sie die richtige IP-Adresse zuweisen).
- Ist das Feld **Bevorzugter DNS Server** noch leer, wählen Sie die Checkbox **Folgende DNS-Serveradressen verwenden** und tragen Sie die IP-Adresse Ihres OpenComNet 20 (im Auslieferungszustand 192.168.1.1) ein. Klicken Sie dann auf **OK**.

Internetzugang

Vorbereitung Ihrer PCs für den Zugang zum Internet über den OpenComNet 20.

- Stellen Sie sicher, dass das DSL Modem und alle anderen Teile des Netzwerkes die ständig miteinander verbunden sind einwandfrei funktionieren.
- Nachfolgend wird gezeigt wie Sie mit Ihren Browser einen Zugang zum Internet über das lokale Netzwerk LAN herstellen.

Windows 98 SE/2000

- Klicken Sie im Startmenü auf -> Einstellungen -> Systemsteuerung.
- Wählen Sie **Internet**.
- Wählen Sie die Registerkarte **Verbindungen** und klicken Sie dann auf **Setup**.
- Wählen Sie **Manuelle Einrichtung der Internetverbindung ...** und klicken Sie dann auf **Weiter**.
- Wählen Sie **Internetverbindung über ein lokales Netzwerk (LAN)** und klicken Sie auf **Weiter**.
- Wählen Sie **Automatische Suche des Proxyservers** und klicken Sie auf **Weiter**.
- Wählen Sie z. B. „Ja“ bei der Frage, ob Sie ein E-Mail Konto erstellen möchten und klicken Sie auf **Weiter**.
- Geben Sie Ihren Namen ein und klicken Sie auf **Weiter**.
- Geben Sie Ihre E-Mail Adresse ein und klicken Sie auf **Weiter**.
- Geben Sie die Namen der Posteingangs- und ausgangsserver an (z. B. bei AOL: smtp.de.aolcom und imap.de.aol.com) und klicken Sie auf **Weiter**.
- Geben Sie Kontonamen und Kennwort an und klicken Sie auf **Weiter**.
- Klicken Sie auf **Fertig stellen**; damit ist die Einrichtung beendet.

Windows XP

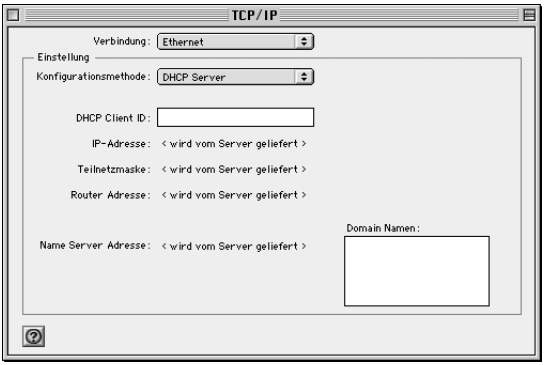
- Klicken Sie im Startmenü auf -> Systemsteuerung -> Netzwerkverbindungen.
- Wählen Sie „Neue Verbindung erstellen“.
- Schließen Sie das Fenster „Standort Informationen“.
- Klicken Sie auf **Weiter** im Fenster „Assistent für neue Verbindungen“.
- Wählen Sie **Verbindung mit dem Internet herstellen** und klicken Sie auf **Weiter**.
- Wählen Sie **Verbindung manuell einrichten** und klicken Sie auf **Weiter**.
- Prüfen Sie ob **Verbindung über eine beständige Breitbandverbindung herstellen** aktiviert ist und klicken Sie auf **Weiter**.
- Klicken Sie auf **Fertig stellen**, damit ist die Einrichtung beendet.

Macintosh Clients

Der Zugang zum Internet mit Ihrem Macintosh und dem OpenComNet 20 erfolgt in dieser Reihenfolge:

- Mac OS

- Öffnen Sie das Kontrollfeld TCP/IP.



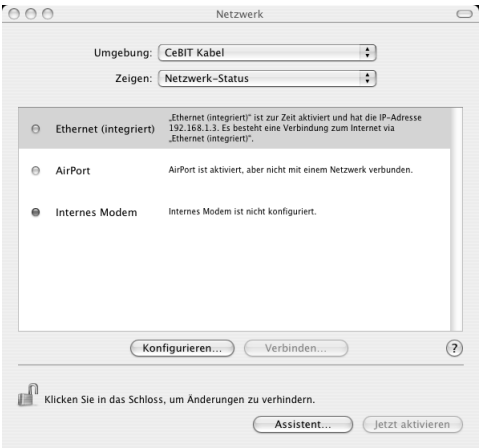
- Wählen Sie **Ethernet** im Feld „Verbindung".
- Wählen Sie **DHCP Server** im Feld „Konfigurationsmethode". Das Feld „DHCP Client ID" bleibt leer.
- Schließen Sie das Kontrollfeld wieder. Die Einstellungen sind gespeichert.

Wenn Sie feste IP Adressen anstelle von DHCP einsetzen erfordert das einige Änderungen:
- Tragen Sie in das Feld „Router Adresse:" die IP Adresse von OpenComNet 20 ein.
- Prüfen Sie die DNS Angaben.

- Mac OS X

- Öffnen Sie über Systemeinstellungen **Netzwerk** .

- Öffnen Sie das Menü **Zeigen**.
- Wählen Sie **Ethernet (integriert)**.


Netzwerk
Umgebung: CeBIT Kabel
Zeigen: Netzwerk-Status
Ethernet (integriert)
„Ethernet (integriert)" ist zur Zeit aktiviert und hat die IP-Adresse 192.168.1.3. Es besteht eine Verbindung zum Internet via „Ethernet (integriert)".
AirPort
AirPort ist aktiviert, aber nicht mit einem Netzwerk verbunden.
Internes Modem
Internes Modem ist nicht konfiguriert.
Konfigurieren...
Verbinden...
Klicken Sie in das Schloss, um Änderungen zu verhindern.
Assistent...
Jetzt aktivieren

- Klicken Sie auf **TCP/IP** und wählen Sie **DHCP** aus.

- Schließen Sie das Fenster und sichern Sie die neuen Einstellungen.

Hinweis

Wollen Sie manuell eingegebene IP-Adressen anstelle von DHCP benutzen, werden folgende Änderungen notwendig:

- Geben Sie im Feld **Router Address** die IP-Adresse vom OpenComNet 20 ein.
- Prüfen Sie die DNS Einstellungen.

Linux Clients

Um einen Internetzugang mit dem OpenComNet 20 herzustellen, ist es nur notwendig den Router als Gateway einzusetzen.

Stellen Sie sicher, dass Sie den Status „root“ haben, bevor Sie mit den Änderungen beginnen.

- Feste IP-Adresse

Standardmäßig nutzen viele Unix Systeme feste IP-Adressen. Wollen Sie das auch weiterhin, müssen Sie folgende Anpassungen vornehmen:
- Tragen Sie als „Default Gateway“ die IP-Adresse vom OpenComNet 20 ein.
- Prüfen Sie die DNS Einstellungen auf Ihrem System.

- Als DHCP-Client (wird empfohlen)

Die folgende Prozedur kann in Teilen abweichen, abhängig ob Linux oder X-windows shell als Oberfläche genutzt wird.
- Starten Sie als X Windows Client.
- Wählen Sie Control Panel -> Network.
- Die „Interface“ Einstellung Ihrer Netzwerkkarte sollte **eth0** sein.
- Klicken Sie auf **Edit** und wählen Sie unter „protocol“ **DHCP** aus, sichern Sie die Einstellungen.
- Damit die Änderungen wirksam werden:
  Benutzen Sie **Deactivate** oder **Activate** wenn verfügbar.
  oder führen Sie einen Neustart durch.

Andere auf Unix basierende Betriebssysteme

Internetzugang über OpenComNet 20:
- Im Eintrag „Gateway“ Ihrer Netzwerkkarte muss die IP-Adresse vom OpenComNet 20 stehen.
- Prüfen Sie die DNS Einstellungen Ihres Systems.

Konfiguration des OpenComNet 20

In diesem Kapitel erhalten Sie Informationen zu folgenden Teilen:

- Internet Zugang
- Konfiguration für das lokale Netzwerkes (LAN)
- Sicherheitseinstellungen

Hinweis

In einigen Fällen kann es erforderlich sein die PCs in Ihrem Netzwerk anzupassen.

Darüber hinaus können noch weitere Konfigurationen nötig sein, dies ist abhängig von den genutzten Leistungsmerkmalen und Funktionen. Eine Übersicht zeigt die nachfolgende Tabelle.

Maßnahme	**siehe unter Kapitel**
Nutzung der folgenden Funktionen:	
• Web-Konfigurator Assistent Konfigurator System-Info	Konfiguration
• Konfigurator Internet System Konten LAN NAT Sicherheit	Konfiguration
• System-Info Status Logbuch	Besondere Leistungsmerkmale
• Telefonanwendung CAPI/TAPI-Treiber installieren CAPIControl HomeNet Control	Konfiguration Telefonanwendung
• Kommunikationssoftware WinSuite	Kommunikationssoftware installieren

Werkseinstellungen

Benutzername:	admin
DHCP-Server:	aktiv
DHCP-Adressenbereich:	192.168.1.002 – 192.168.1.254
Domain-Name:	"local.lan"
DSL-Datenvolumen:	2000 MB
DSL-Einwahl erlauben:	aus
DSL-Volumenkonto:	aus
DSL-Zeitkonto:	aus
DSL-Zeitvolumen:	40 Stunden
DSL-Zugangsdaten:	kein Provider ausgewählt
Entdecken von Angriffen:	aktiv
Firewall:	aktiv
IP-Adresse OpenComNet 20 (LAN):	192.168.1.1
ISDN-Fallback -Datenvolumen:	500 MB
ISDN-Fallback erlauben:	aus
ISDN-Fallback -Volumenkonto:	aus
ISDN-Fallback -Zeitvolumen:	10 Stunden
ISDN-Fallback-Zeitkonto:	aus
ISDN-Zugangsdaten:	keine Einträge
Kennwort:	0000
Leasetime:	3600 Sekunden (entspricht 1 Stunde)
Leerlaufzeit:	5 Minuten
Logbuch:	keine Einträge
OpenComNet 20 ist Default Gateway:	aktiv
OpenComNet 20 ist DNS Server:	aktiv
Routen:	keine Einträge
Sicherheitsstufe:	mittel
SNTP-Zeitserver:	ptbtime1.ptb.de
Subnetzmaske:	255.255.255.0
TCP/IP:	DHCP
Uhrzeit:	Systemuhr - nicht gesetzt
Uhrzeit autom. synchronisieren alle:	2 Stunden
Uhrzeit Synchronisationsabbruch nach:	5 Sekunden
Uhrzeit Synchronisationsversuche:	2
Uhrzeit Synchr. nur bei vorh. Internetverb.:	aktiv
Datum:	nicht gesetzt
Virtueller Server:	nicht aktiv
WAN IP-Adresse:	0.0.0.0
Zeitzohne:	MET

Der Assistent

Ein HTTP Server ist Bestandteil des OpenComNet 20. Das ermöglicht eine einfache Verbindung und Konfiguration des Routers mit einem Internet Browser. Der Browser muss JavaScript unterstützen. Das Konfigurationsprogramm sollte mit folgenden Browsern funktionieren:

- Internet Explorer ab Vers. 6.0
- Netscape ab Vers. 7.0
- Opera ab Vers. 7.0
- Mozilla ab Vers. 1.4
- Safari 1.2

Vorbereitungen

Bevor Sie mit der Konfiguration beginnen, stellen Sie folgendes sicher:

- dass alle Rechner gemäß dem vorangegangenen Kapitel „PC Konfiguration“ konfiguriert wurden.
- Fahren Sie alle Rechner im LAN herunter und schalten Sie sie **aus**.
- Schalten Sie erst Ihren OpenComNet 20 ein und **danach** auch die angeschlossenen Rechner.

So benutzen Sie Ihren Browser

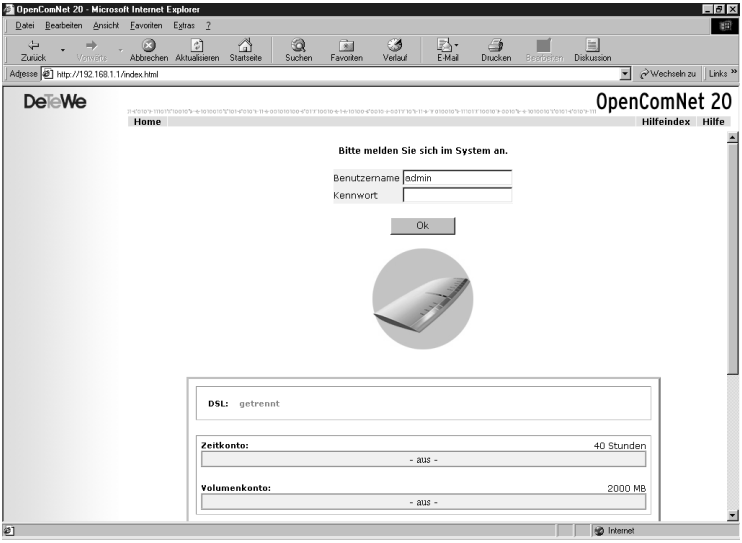
Um eine Verbindung zwischen Rechner und OpenComNet 20 herzustellen:

1. Starten Sie den Browser an einem der angeschlossenen Rechner.
2. Ins Adressfenster geben Sie „HTTP://“ ein und dann die Adresse vom OpenComNet 20, verwenden Sie die werksseitig eingestellte Adresse.

192.168.1.1

oder

opencomnet_20.local.lan



Sie werden aufgefordert, **Benutzername** und **Kennwort** einzugeben:

Benutzername admin
Kennwort (bei Auslieferung) 0000

Klicken Sie auf **OK**.

Kommt es jetzt zu keinem Verbindungsaufbau, prüfen Sie folgendes:

- OpenComNet 20 ist vollständig und korrekt installiert und in Betrieb. Sie können die Verbindung durch Aussenden eines Testsignals prüfen.

  Schalten Sie den PC in den MS-DOS Mode zurück und geben Sie in der Befehlszeile folgendes ein:

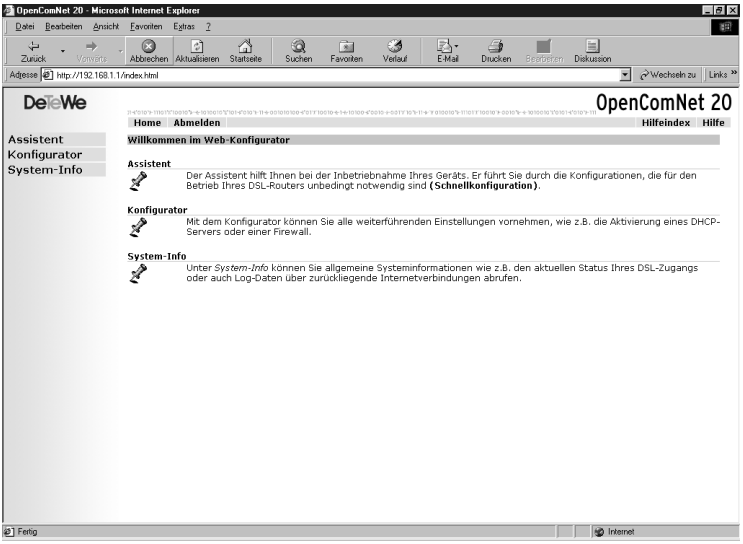
  ping 192.168.1.1

- Erhalten Sie keine Antwort (weil die Verbindung nicht besteht oder die IP-Adresse des PCs nicht mit der des Routers kompatibel ist), gehen Sie folgendermaßen vor:
  Benutzt Ihr PC eine feste IP-Adresse muss diese im Bereich 192.168.1.2 und 192.168.1.254 liegen um kompatibel mit der werkseitig eingestellten IP-Adresse 192.168.1.1 des Routers zu sein. Ebenfalls muss die Einstellung der Netzwerkmaske auf 255.255.255.0 gesetzt sein. Näheres finden Sie im Kapitel - PC Konfiguration - unter dem Begriff „TCP/IP Einstellungen“.

- Prüfen Sie ob der PC und der OpenComNet 20 sich in einem Netzwerk befinden.
- Prüfen Sie ob der aktuelle Treiber für Ihre Netzwerkkarte benutzt wird.
- Prüfen Sie die gesamte Verkabelung.

Hinweis

Die Verbindung zum Web-Konfigurator wird von einem Timer überwacht und nach 20 Minuten Leerlauf automatisch getrennt.


OpenComNet 20 - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Bearbeiten Diskussion
Adresse http://192.168.1.1/index.html
Wechseln zu Links
DeTeWe
OpenComNet 20
Home Abmelden
Hilfeindex Hilfe
Assistent
Konfigurator
System-Info
Willkommen im Web-Konfigurator
Assistent
Der Assistent hilft Ihnen bei der Inbetriebnahme Ihres Geräts. Er führt Sie durch die Konfigurationen, die für den Betrieb Ihres DSL-Routers unbedingt notwendig sind (Schnellkonfiguration).
Konfigurator
Mit dem Konfigurator können Sie alle weiterführenden Einstellungen vornehmen, wie z.B. die Aktivierung eines DHCP-Servers oder einer Firewall.
System-Info
Unter System-Info können Sie allgemeine Systeminformationen wie z.B. den aktuellen Status Ihres DSL-Zugangs oder auch Log-Daten über zurückliegende Internetverbindungen abrufen.
Fertig
Internet

Das Hauptmenü im linken Teil enthält Schaltflächen zu weiteren häufig gebrauchten Eingabefenstern.

Das Hauptmenü enthält auch die beiden Schaltflächen:

- **Abmelden** haben Sie alle Einstellungen erledigt, klicken Sie auf **Abmelden**.
- **Home** Durch Klick auf **Home** springen Sie von einer beliebigen Seite zurück auf diese Startseite

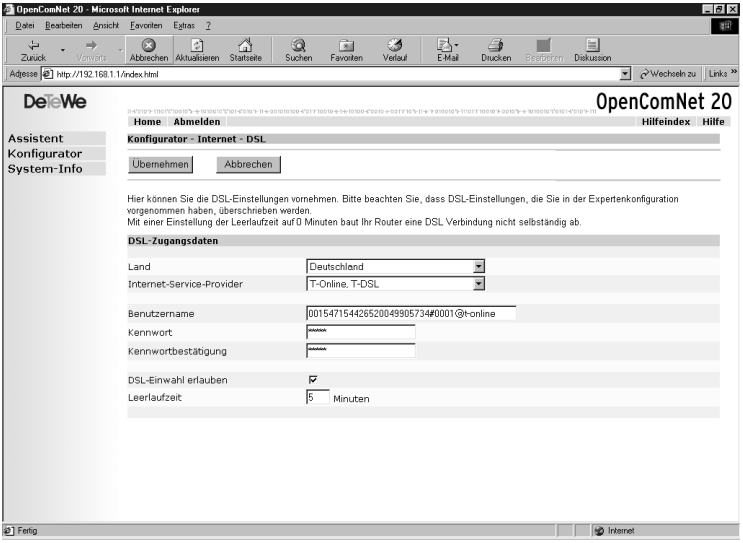
Navigieren im Menü und Dateneingabe

- Benutzen Sie die linke Spalte mit den Schaltflächen oder auch die Funktion **Zurück** im Fenster des Browsers.
- Wechseln Sie zwischen den Bildschirmen und haben vorher Einstellungen verändert, werden diese nicht gesichert. Bevor Sie einen Bildschirm verlassen, müssen Sie die geänderten Einstellungen durch Klick auf die entsprechende Schaltfläche **Übernehmen** speichern.

Hinweis

In jedem Eingabefenster finden Sie **Hilfe**. Hier finden Sie Hilfetexte zum aktuellen Bildschirm.

Assistent



Land — Wählen Sie das Land aus in dem sich Ihr Standort befindet.

Internet Service Provider — Die Liste enthält eine Auswahl der in dem von Ihnen gewählten Land gebräuchlichsten Anbietern.

- Wählen Sie hier aus der Liste den Serviceprovider aus, mit dem Sie einen Netzzugangsvertrag abgeschlossen haben. Ist Ihr Provider nicht aufgeführt wählen Sie „Andere Provider“.

Hinweis

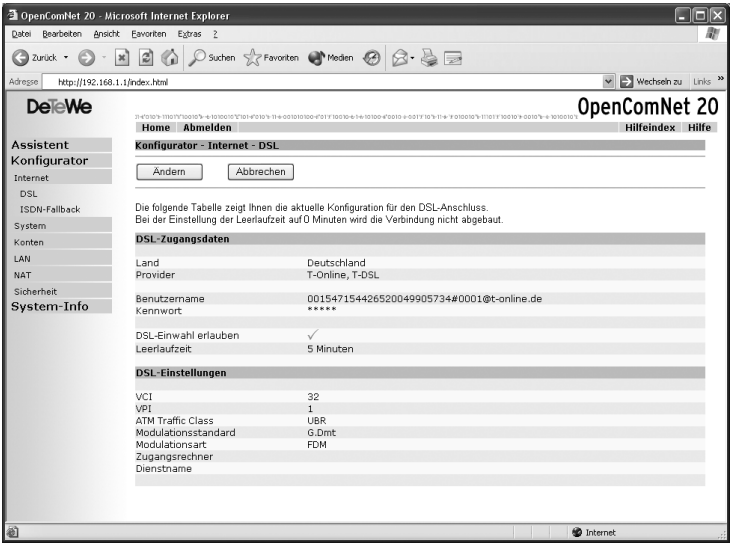
Die Parameter Ihres im OpenComNet 20 integrierten DSL-Modems werden hierdurch automatisch auf die Erfordernisse Ihres Serviceproviders angepasst. Sollte Ihr Provider sehr neu und daher hier nicht aufgelistet sein, müssen Sie die notwendigen Einstellungen manuell vornehmen, siehe Seite 28/29. Sie brauchen hierzu die Verbindungsdaten von Ihrem Internetprovider.

Benutzername	Tragen Sie hier den vereinbarten Benutzernamen ein. • Format des Benutzernames (ohne Leerzeichen): T-Online: [Anschlusskennung][T-Online-Nummer] # [Mitbenutzernummer]@t-online.de. AOL: [AOL-Benutzername]@de.aol.com. Bei AOL muss zusätzlich die MTU auf 1400 reduziert werden (siehe **Konfigurator / LAN / DHCP / Server ändern**, Seite 57/58).
Kennwort	Tragen Sie das vereinbarte Kennwort ein.
Kennwort-bestätigung	Wiederholen Sie das Kennwort.
DSL- Einwahl erlauben	Aktivieren Sie die Einstellung mit ✔.
Leerlaufzeit	Tragen Sie einen Wert größer 0 ein. Nach dem Erreichen der Leerlaufzeit trennt der Router die Internetverbindung. Wenn hier 0 eingetragen wird ist die Leerlaufzeitüberwachung für Internetverbindungen abgeschaltet.

Klicken Sie auf **Übernehmen**.

Hinweis

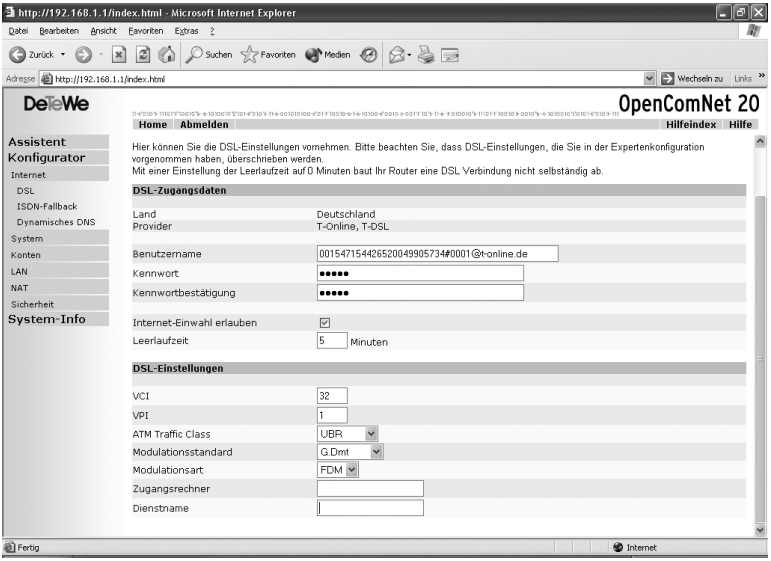
Wenn Sie den OpenComNet 20 lediglich als ISDN-Router einsetzen wollen müssen Sie trotzdem Blind-Eingaben für einen DSL-Zugang machen, z. B. Benutzername „Test“ und Kennwort „Test“. Markieren Sie die Checkbox „DSL Einwahl erlauben“ und stellen Sie die gewünschte Leerlaufzeit ein. Diese gilt gleichermaßen für ISDN-Verbindungen. Geben Sie danach Ihre Zugangsdaten für ISDN-Fallback unter **Konfigurator / Internet / ISDN-Fallback** ein, s. Seite 33.



Sie sehen jetzt die Zusammenfassung aller Zugangsdaten. Damit endet der Assistent. Klicken Sie nur dann auf **Ändern**, wenn Sie noch etwas korrigieren wollen.

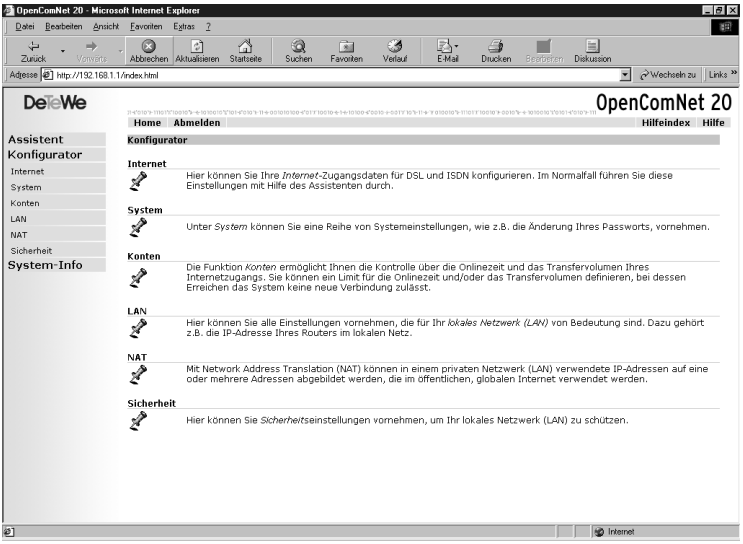
Hinweis

Die in dieser Maske aufgelisteten DSL-Einstellungen wurden automatisch bei Ihrer Providerauswahl (siehe vorherige Maske) generiert.
Wenn Ihr Wunschprovider dort nicht angeboten wurde, können hier über **Ändern** die notwendigen Einstellungen auch manuell vorgenommen werden.
Hierzu müssen Sie vorher die erforderlichen DSL-Einstellungen bei Ihrem Provider erfragen.



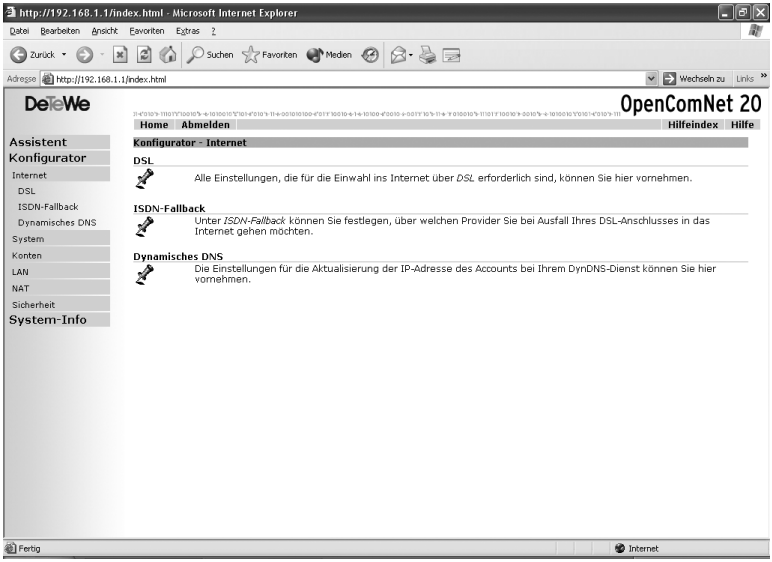
Wenn Sie alle Angaben gemacht haben, klicken Sie auf **Übernehmen**.

Der Konfigurator


OpenComNet 20 - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Bearbeiten Diskussion
Adresse http://192.168.1.1/index.html
Wechseln zu Links
DeTeWe
OpenComNet 20
Home Abmelden
Hilfeindex Hilfe
Assistent
Konfigurator
Internet
System
Konten
LAN
NAT
Sicherheit
System-Info
Konfigurator
Internet
Hier können Sie Ihre Internet-Zugangsdaten für DSL und ISDN konfigurieren. Im Normalfall führen Sie diese Einstellungen mit Hilfe des Assistenten durch.
System
Unter System können Sie eine Reihe von Systemeinstellungen, wie z.B. die Änderung Ihres Passworts, vornehmen.
Konten
Die Funktion Konten ermöglicht Ihnen die Kontrolle über die Onlinezeit und das Transfervolumen Ihres Internetzugangs. Sie können ein Limit für die Onlinezeit und/oder das Transfervolumen definieren, bei dessen Erreichen das System keine neue Verbindung zulässt.
LAN
Hier können Sie alle Einstellungen vornehmen, die für Ihr lokales Netzwerk (LAN) von Bedeutung sind. Dazu gehört z.B. die IP-Adresse Ihres Routers im lokalen Netz.
NAT
Mit Network Address Translation (NAT) können in einem privaten Netzwerk (LAN) verwendete IP-Adressen auf eine oder mehrere Adressen abgebildet werden, die im öffentlichen, globalen Internet verwendet werden.
Sicherheit
Hier können Sie Sicherheitseinstellungen vornehmen, um Ihr lokales Netzwerk (LAN) zu schützen.
Internet

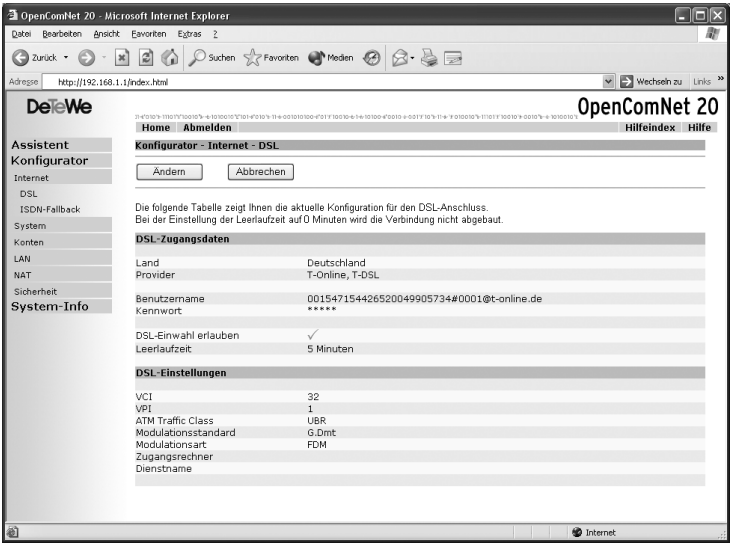
Internet	Hier können Sie die Internet Zugangsdaten für DSL und ISDN konfigurieren.
System	Systemeinstellungen ändern, wie z. B. Passwort.
Konten	Die Funktion ermöglicht die Kontrolle über die Onlinezeit und das Transfervolumen des Internetzugangs.
LAN	Einstellungen, die Ihr lokales Netzwerk betreffen, wie z. B. IP-Adressen.
NAT	Einstellungen, die es erlauben, IP-Adressen eines privaten Netzwerkes in IP-Adressen für das öffentliche, globale Internet umzusetzen.
Sicherheit	Sicherheitseinstellungen für Ihr lokales Netzwerk.

Internet



DSL	Einstellungen, die für die Einwahl ins Internet über DSL erforderlich sind.
ISDN-Fallback	Festlegen über welchen Provider ins Internet gegangen wird, wenn der DSL Anschluss einmal ausgefallen sein sollte.
Dynamisches DNS	Einstellung für die Parameter Ihres Accounts beim DynDNS-Dienst.

DSL

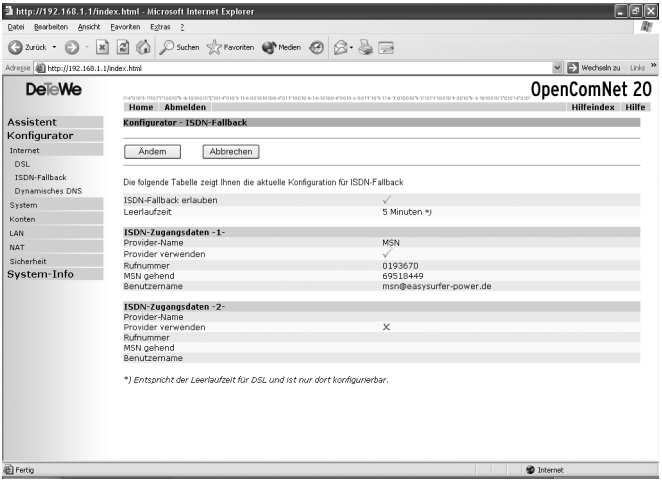


Sie sehen jetzt die Zusammenfassung aller Zugangsdaten. Klicken Sie nur dann auf **Ändern**, wenn Sie noch etwas korrigieren wollen.

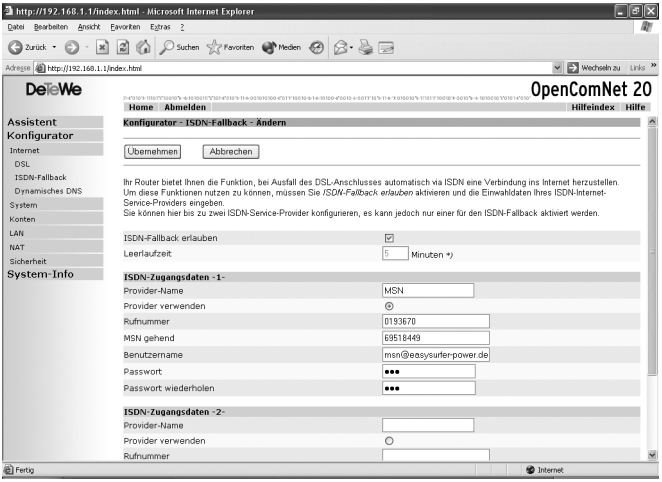
Hinweis

Die in dieser Maske aufgelisteten DSL-Einstellungen wurden automatisch bei Ihrer Providerauswahl generiert.
Wenn Ihr Wunschprovider dort nicht angeboten wurde, können hier über **Ändern** die notwendigen Einstellungen auch manuell vorgenommen werden.
Hierzu müssen Sie vorher die erforderlichen DSL-Einstellungen bei Ihrem Provider erfragen.

ISDN-Fallback



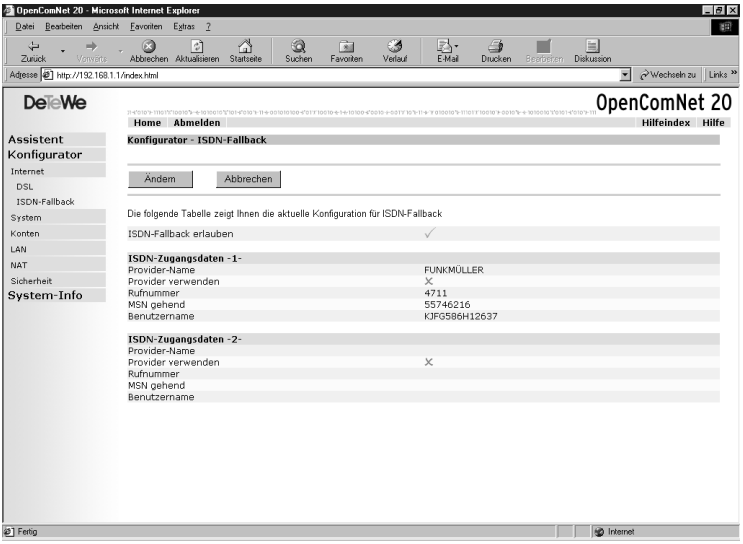
Wenn Sie für den Fall, dass Ihr DSL-Provider ausfallen sollte oder Sie keinen DSL-Zugang nutzen wollen, einen ISDN-Provider konfigurieren möchten, klicken Sie hier auf **Ändern**.



Aktivieren Sie die Checkbox - ISDN Fallback erlauben - ✔ .
Tragen Sie alternative ISDN-Provider Ihrer Wahl ein.
Markieren Sie Ihren bevorzugten „Rückfallprovider“, indem Sie die Checkbox **Provider verwenden** aktivieren ✔.
Klicken Sie auf **Übernehmen**.

Hinweis

Der Rückfall auf den von Ihnen konfigurierten ISDN-Provider erfolgt bei DSL-Ausfall automatisch. Der Router kann jedoch nicht erkennen, wann DSL ggf. wieder verfügbar ist. Wenn Sie jedoch die Verbindung ins Internet trennen, wird bei Neuaufbau automatisch erst wieder DSL probiert. Sie können feststellen ob DSL wieder verfügbar ist, indem Sie die DSL-Sync LED beobachten. Wenn diese LED leuchtet ist DSL wieder verfügbar.



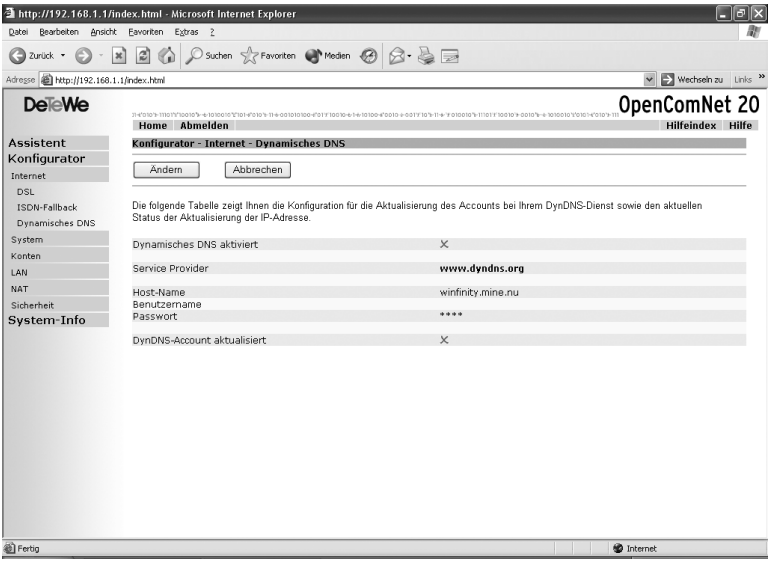
Sie sehen jetzt die Zusammenfassung aller Daten. Klicken Sie nur dann auf **Ändern**, wenn Sie noch etwas korrigieren wollen.

Dynamisches DNS

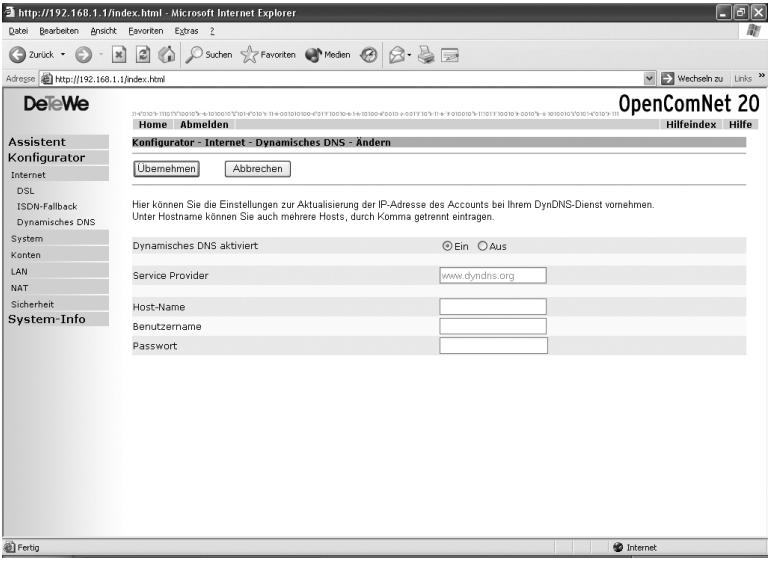
Dieser kostenlose Service ist sehr nützlich in Verbindung mit der Anwendung „Virtueller Server". Er erlaubt den Zugriff aus dem Internet auf den „Virtueller Server" unter Verwendung eines URL (Uniform Ressource Locator), genauso wie über eine normale IP-Adresse.
Damit wird gleichzeitig das Problem der dynamischen Internetadresse gelöst. Bei dem Einsatz dynamischer IP-Adressen wird bei jeder Internetverbindung die aktuelle IP-Adresse geändert und es ist somit schwierig bis unmöglich, Verbindungen zu Ihrem Netz herzustellen.

Der Dynamische DNS Service arbeitet nach folgendem Prinzip:

- Sie müssen sich für diesen Service unter http://www.dyndns.org anmelden (die Anmeldung ist kostenlos). Sie erhalten Ihr Password dann per E-Mail.
- Nach der Registrierung erhalten Sie unter http://www.dyndns.org / **Dynamic DNS** / **Add Host** Ihren Domain-Namen.
- Tragen Sie anschließend die Daten, die Sie von www.dyndns.org erhalten haben, im OpenComNet 20 ein. Verwenden Sie dazu das Eingabefenster „Dynamisches DNS".
- Der OpenComNet 20 wird jetzt automatisch sicherstellen, dass Ihre IP-Adresse bei www.dyndns.org aufgenommen ist.
- Internetnutzer haben bei aktiviertem DynDNS die Möglichkeit Ihren **Virtuellen Server** (oder DMZ-PC) auch unter dem Domainnamen anzusprechen.



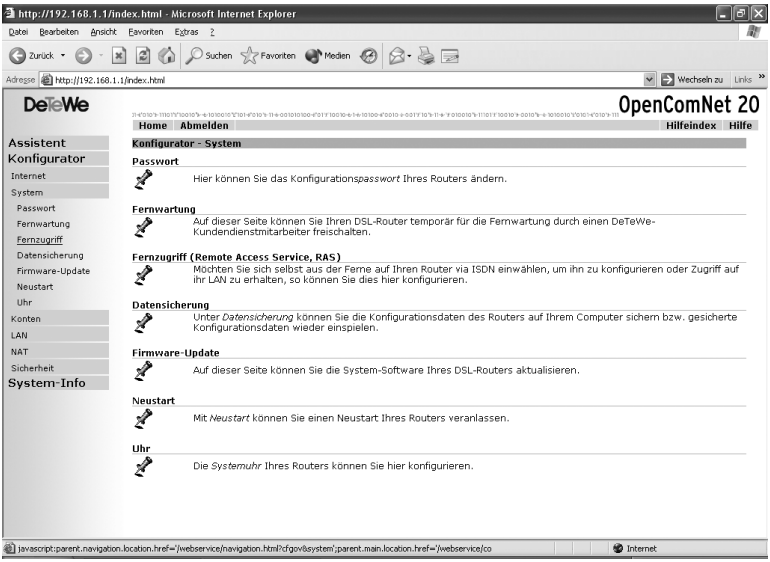
Wollen Sie Dynamisches DNS aktivieren/deaktivieren bzw. Änderungen an den Einstellungen vornehmen klicken Sie auf **Ändern**.



Markieren Sie die Checkbox **Ein** um Dynamisches DNS zu aktivieren.
Als **Service Provider** ist www.dyndns.org fest voreingestellt.
Tragen Sie unter **Host-Name** den Domainnamen ein, der Ihnen vom DynDNS-Service zugeteilt wurde. Haben Sie mehrere Namen, können Sie einen aussuchen.
Tragen Sie unter **Benutzernamen** Ihren Benutzernamen für den DynDNS-Service ein.
Tragen Sie unter **Passwort** das dazugehörige Passwort ein.
Klicken Sie nach Beendigung der Eingaben auf **Übernehmen**.

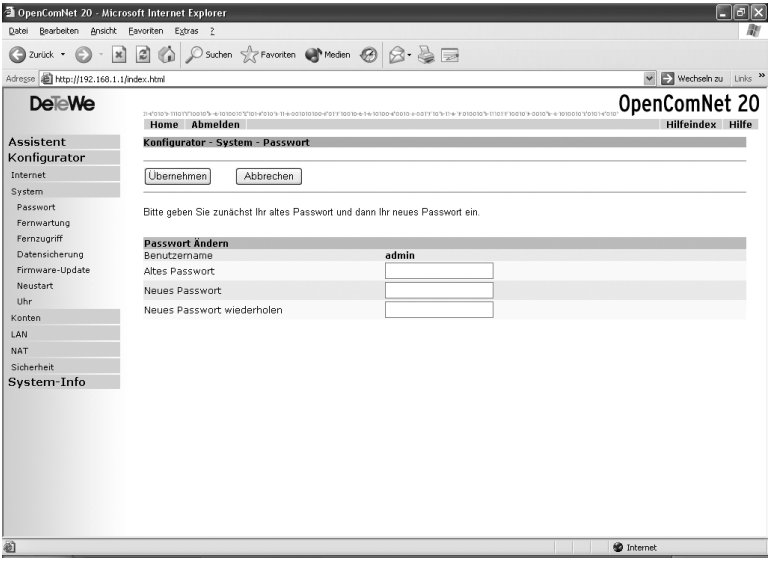
Eine erfolgreiche Aktualisierung des DynDNS-Accounts erkennen Sie am grünen Häkchen in der Zeile **DynDNS-Account aktualisiert** (Abb. siehe umseitig). Erscheint dort allerdings ein rotes „x“, dann überprüfen Sie Ihre Eingaben. Eventuell stimmt z. B. der Host-Name nicht mit dem zugeteilten Host-Namen überein. Verbinden Sie sich erneut mit dem DynDNS Service Provider und beheben Sie das Problem.

System



Passwort	Hier können Sie das Konfigurationspasswort des Routers ändern.
Fernwartung	Freischaltung des Routers für die Fernwartung.
Fernzugriff	Konfiguration der Zugriffsmöglichkeit aus der Ferne auf den Router oder das LAN.
Datensicherung	Sie können die Konfigurationsdaten in eine Datei sichern und die Daten aus der Datei wieder einspielen.
Firmware Update	Aktualisierung der System-Software
Neustart	Veranlasst den Neustart
Uhr	Systemuhr einstellen

Passwort

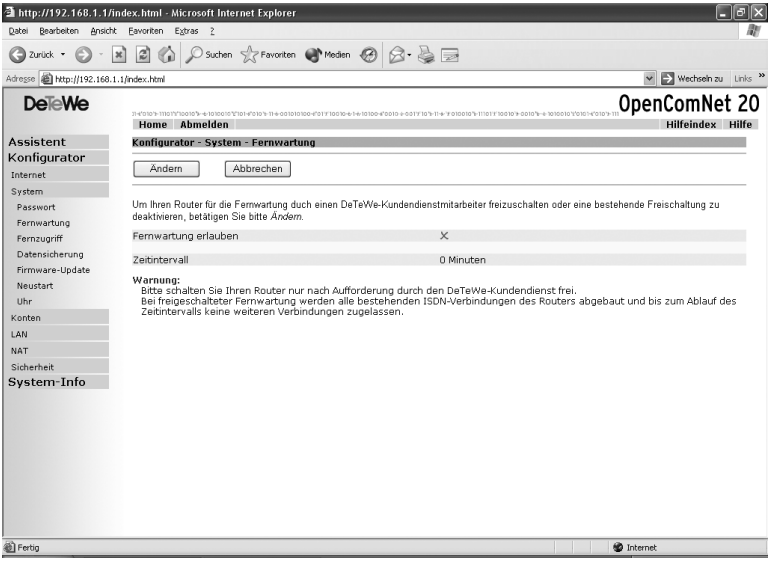


Machen Sie die erforderlichen Angaben in den Feldern:

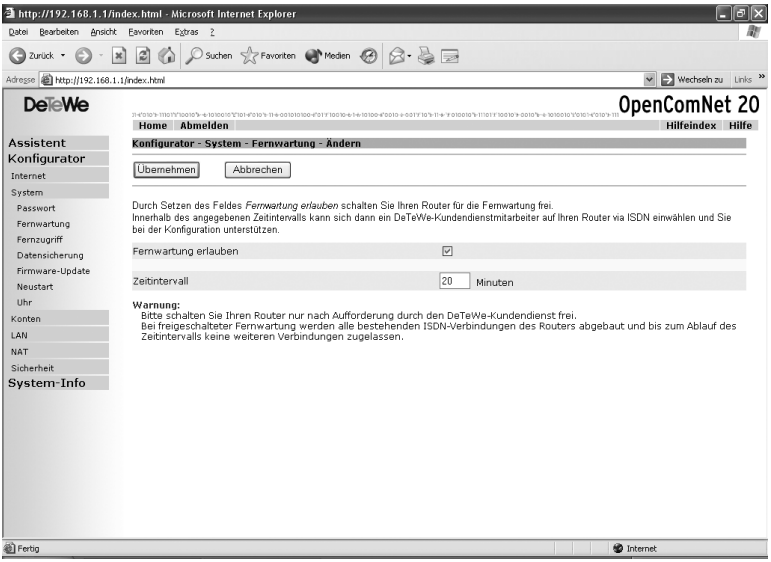
- Altes Passwort
- Neues Passwort (max. 20 stellig)
- Neues Passwort wiederholen

Klicken Sie auf **Übernehmen**.

Fernwartung

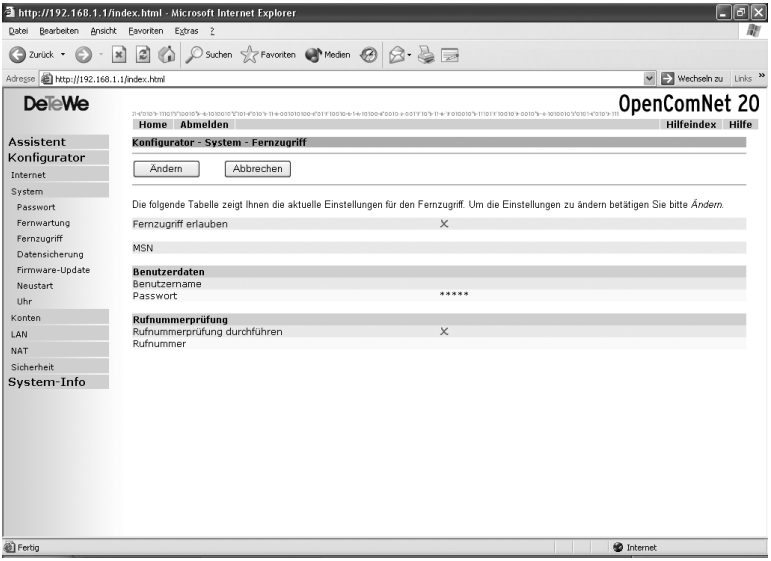


Um die Fernwartung Ihres Routers zu ermöglichen bzw. die Freischaltung nach erfolgter Fernbetreuung zu deaktivieren klicken Sie auf **Ändern**.

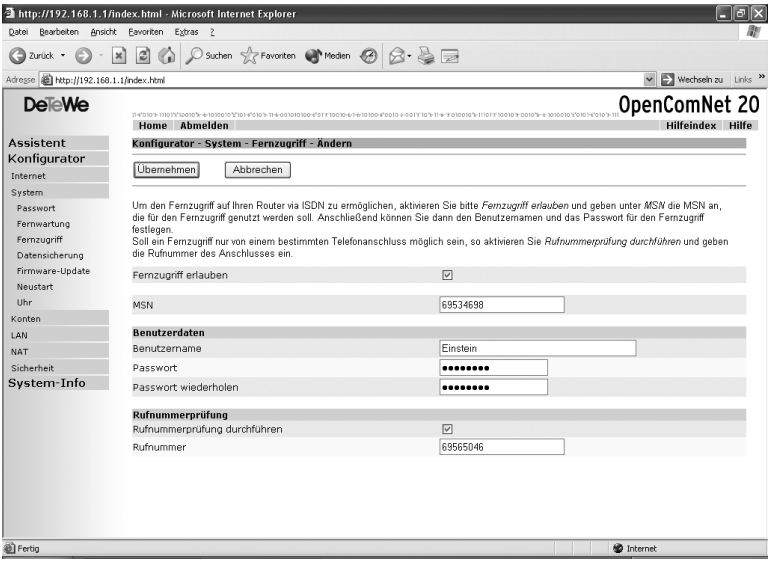


Markieren Sie die Checkbox entsprechend und geben Sie einen Wert für das Zeitintervall ein, in dem der Router für eine Fernwartung erreichbar ist. Klicken Sie auf **Übernehmen**.

Fernzugriff



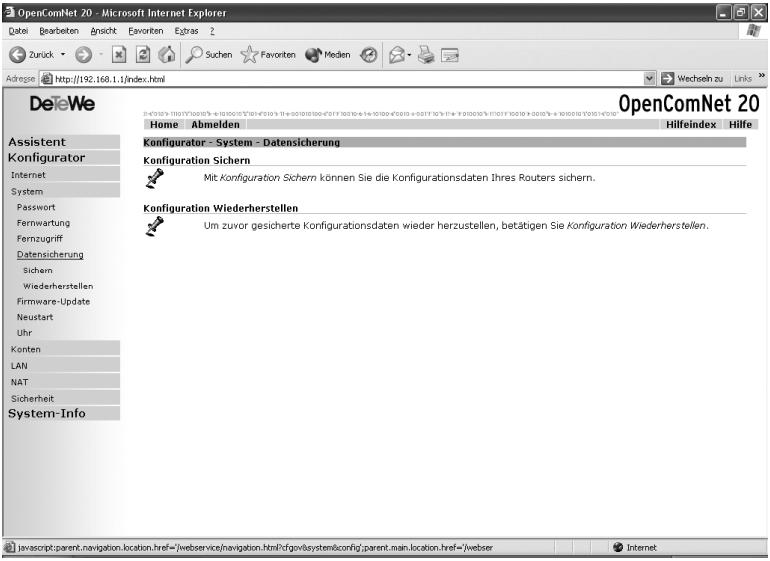
Klicken Sie auf **Ändern** um die Konfiguration der Zugriffsmöglichkeit aus der Ferne auf den Router vorzunehmen.



Markieren Sie die Checkbox und machen Sie die Eingaben in den entsprechenden Feldern. Klicken

Sie auf **Übernehmen**. Auf dem PC, über den Sie per ISDN auf den OpenComNet 20 bzw. Ihr LAN zugreifen wollen, müssen Sie eine DFÜ-Verbindung mit den gleichen Parametern einrichten. Dazu gehört die Anwahl der für den Zugriff eingetragenen MSN sowie korrekte Eingabe des Benutzernamens und des Passwortes.

Datensicherung



Konfiguration sichern	Speichert die Konfigurationsdaten in eine Datei.
Konfiguration wiederherstellen	Lädt eine Datei mit den Konfigurationsdaten.

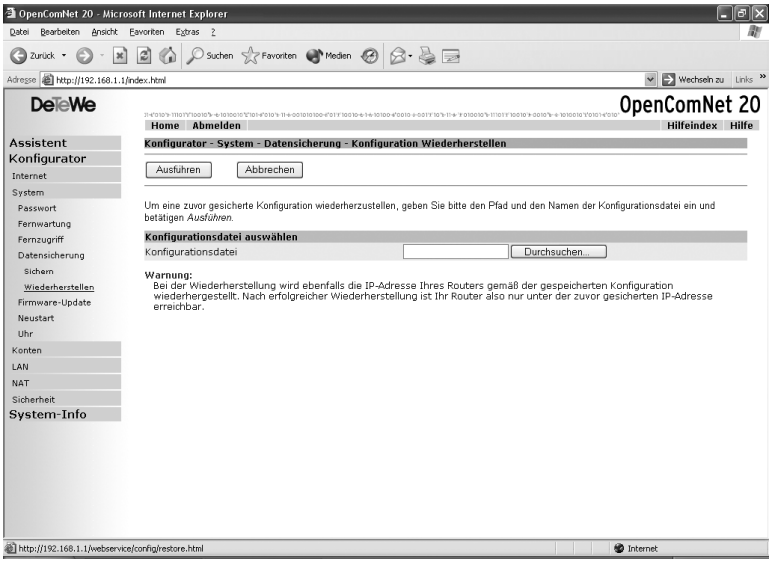
- Konfiguration sichern

Klicken Sie auf **Speichern**.
Sie werden aufgefordert ein Verzeichnis für die Datensicherung zu benennen.

Wählen Sie das Verzeichnis und klicken Sie auf **Speichern**.

Klicken Sie auf **Schließen**.

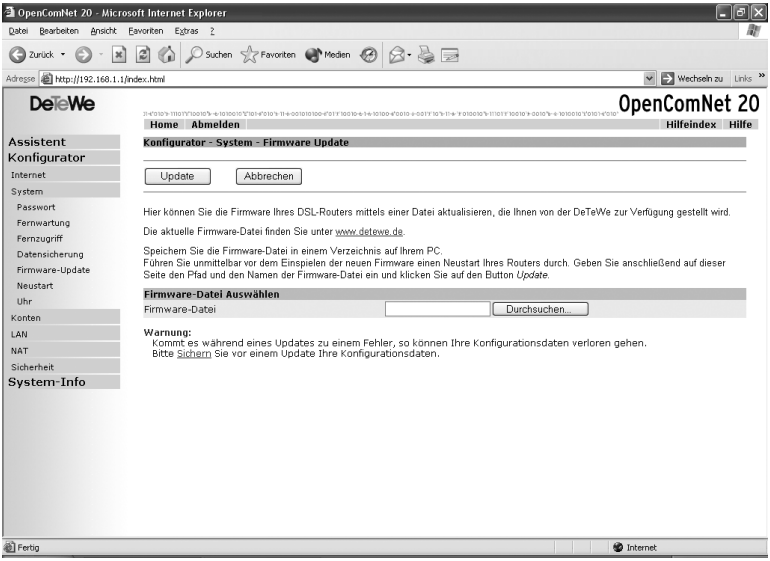
- Konfiguration wiederherstellen



Klicken Sie auf **Durchsuchen** und wählen Sie eine zuvor gespeicherte Konfigurationsdatei aus.

Klicken Sie dann auf **Ausführen**.

Firmware Update



Laden Sie über den angegebenen Link eine neue Firmware von der DeTeWe Internetseite.

Speichern Sie diese Firmware in einem Verzeichnis auf Ihrem Rechner.

Klicken Sie auf **Durchsuchen** und wählen Sie den Pfad für die gerade abgespeicherte neue Firmware (*.tar) aus.

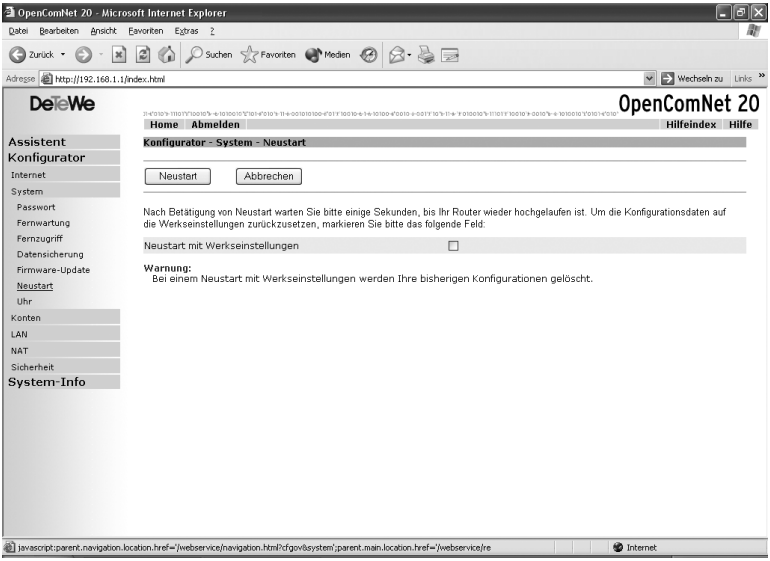
Klicken Sie auf **Update**.

Nach dem Update wird Ihnen ein Neustart angeboten. Dieser ist notwendig, um die neue Firmware in den OpenComNet 20 zu übernehmen.

Hinweis

Bevor Sie eine neue Firmware in den OpenComNet 20 laden, speichern Sie Ihre bisherige Konfiguration auf einem Ihrer Rechner ab.
Machen Sie dann über den RESET-Taster einen Reset **mit** Zurücksetzen auf die Werkseinstellungen.

Neustart

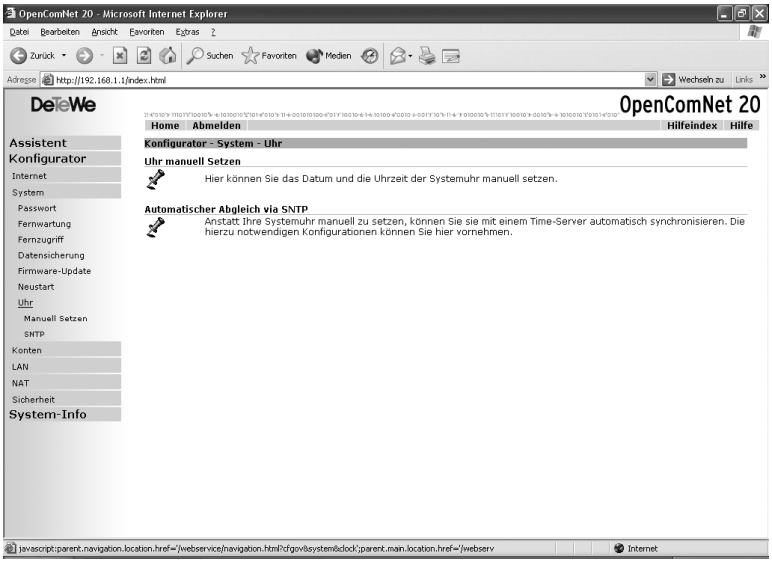


Wollen Sie einen ganz gewöhnlichen Neustart durchführen, klicken Sie einfach auf **Neustart**. Wollen Sie dagegen beim Neustart die Werkseinstellungen laden, aktivieren Sie vorher die Checkbox Neustart mit Werkseinstellungen ✔.

Hinweis

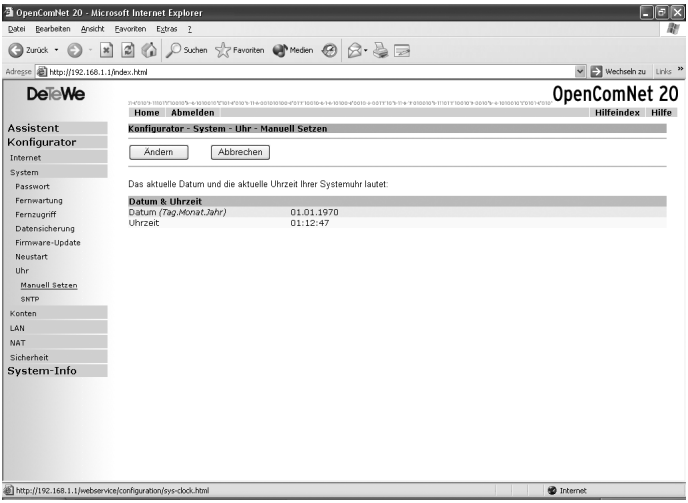
Nach dem Laden einer neuen Firmware sollten Sie sicherheitshalber einen Neustart, besser noch das Zurücksetzen auf die Werkseinstellungen durchführen.

Uhr

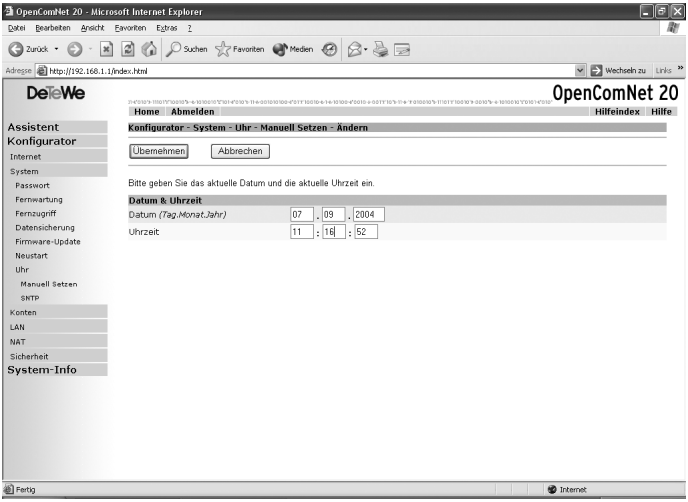


Uhr manuell setzen	Systemuhr des Routers einstellen.
Automatischer Abgleich via SNTP	Die Uhr wird von einem Time Server koordiniert.

- Uhr manuell setzen



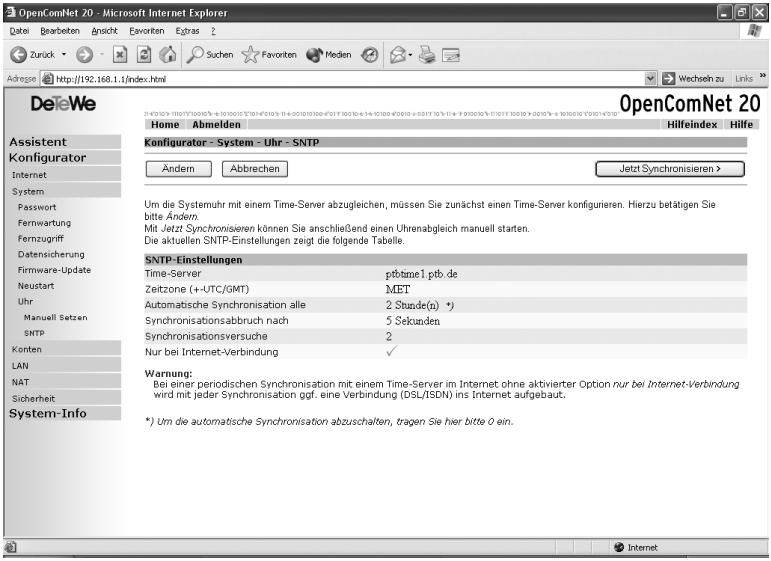
Sie sehen jetzt unter Datum & Uhrzeit die aktuellen Einstellungen. Wenn Sie Änderungen haben, klicken Sie auf **Ändern**.



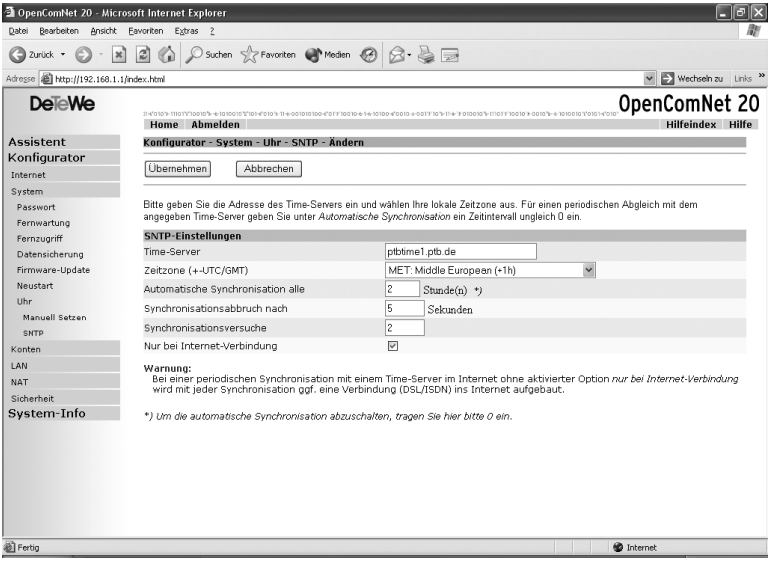
Machen Sie Ihre Angaben in den entsprechenden Feldern nach dem vorgegebenen Schema:
Datum - Tag : Monat : Jahr
und
Uhrzeit - hh : mm : ss

Klicken Sie danach auf **Übernehmen**.

- SNTP



Sie sehen jetzt die aktuellen Einstellungen. Klicken Sie auf **Ändern**, wenn Sie die Konfiguration für den SNTP-Zeitserver ändern wollen. Hiermit können Sie erreichen, dass Ihre Systemuhr automatisch in den vorgegebenen Intervallen über das Internet synchronisiert wird.



Tragen Sie unter **Time Server** einen Internetuhrzeitserver Ihrer Wahl ein.

Wählen Sie die zu Ihrem Wohnort passende Zeitzone und beachten Sie dabei auch die aktuelle Sommer-/Winterzeit-Regelung. Eine automatische Korrektur auf die entsprechende „Saison-Zeit“ erfolgt nicht – wählen Sie eine dementsprechende Zeitzone aus.

Tragen Sie ein, wie oft die Uhrzeit synchronisiert werden soll
(Wertebereich: Alle 0-1000 Stunden).

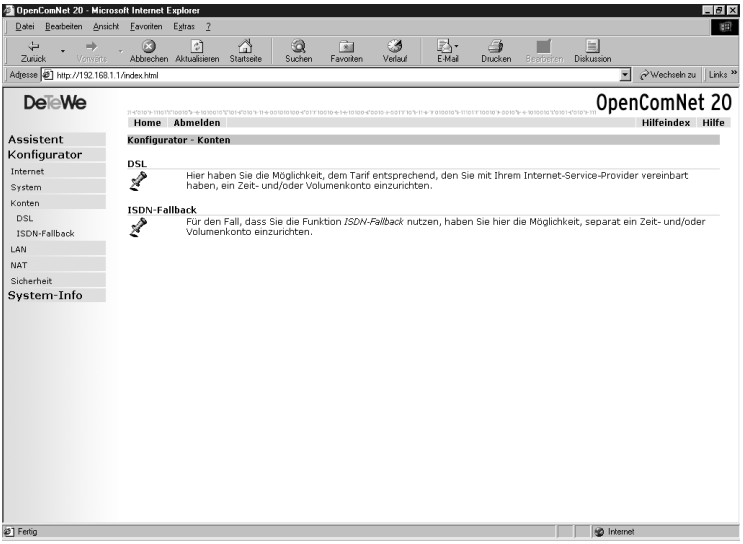
Tragen Sie ein, wann ein Synchronisationsversuch abgebrochen werden soll
(Wertebereich: 0-30 Sekunden).

Tragen Sie ein, wie viele Synchronisationsversuche durchgeführt werden sollen
(Wertebereich: 0-10 Versuche).

Aktivieren Sie die Checkbox - Nur bei Internetverbindung - ✔ findet die Uhrzeitsynchronisation nur dann statt, wenn Sie ohnehin eine Internetverbindung aufgebaut haben.

Klicken Sie auf **Übernehmen**.

Konten



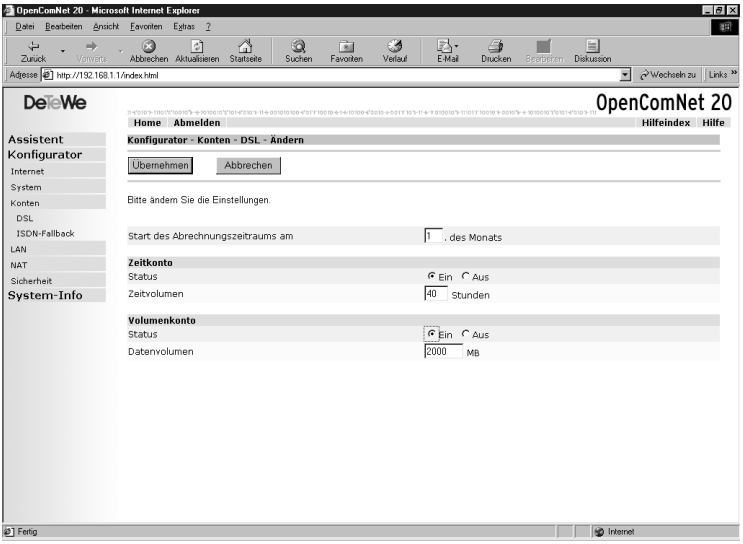
DSL	Einrichtung von Zeit- und/oder Volumenkonten.
ISDN-Fallback	Einrichtung von Zeit- und/oder Volumenkonten für die Funktion ISDN-Fallback.

Hinweis

Wenn Sie ein Zeit- und/oder Volumenkonto konfiguriert haben, wird der Internetzugang in dem Augenblick vom OpenComNet 20 gesperrt, wenn das eingestellte Zeit- oder Volumenlimit erreicht wird. Am 1. des nächsten Monats wird der Internetzugang automatisch wieder freigeschaltet. Wenn Sie das Internet vorher wieder nutzen möchten, müssen Sie das Konto über die Konfiguration zurücksetzen.

DSL

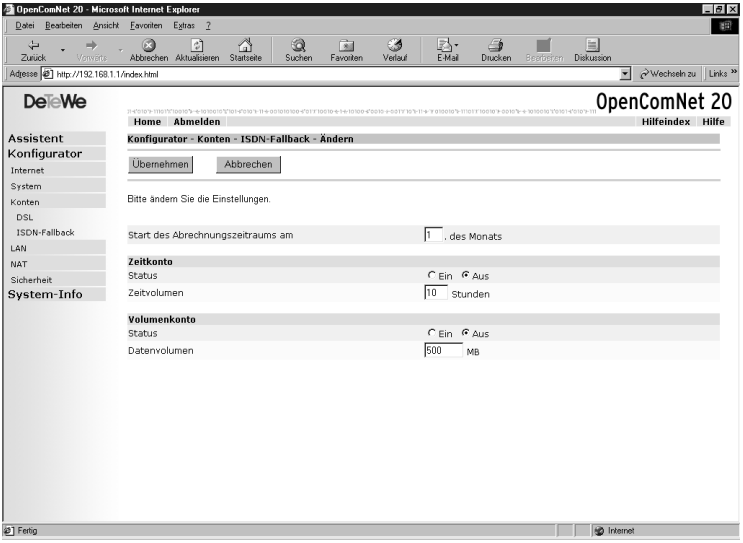
Sie sehen jetzt die aktuellen Einstellungen. Wenn Sie Änderungen vornehmen wollen, klicken Sie auf **Ändern**.



Ändern Sie die Angaben in den Feldern entsprechend Ihren Vorstellungen und klicken Sie auf **Übernehmen**.

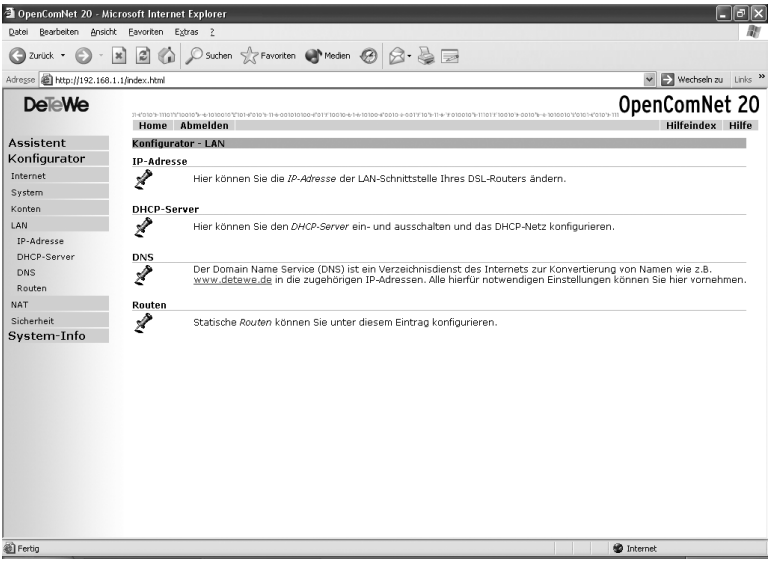
ISDN Fallback

Sie sehen jetzt die aktuellen Einstellungen. Wenn Sie Änderungen haben, klicken Sie auf **Ändern**.



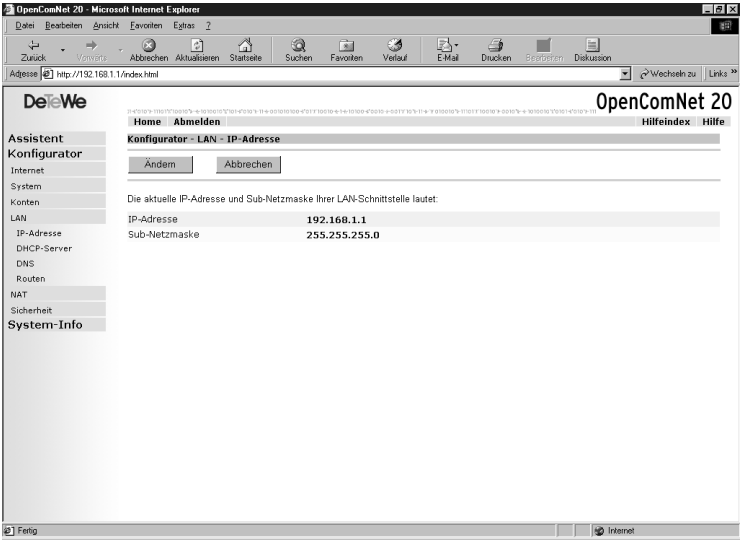
Ändern Sie die Angaben in den Feldern entsprechend Ihren Vorstellungen und klicken Sie auf **Übernehmen**.

LAN

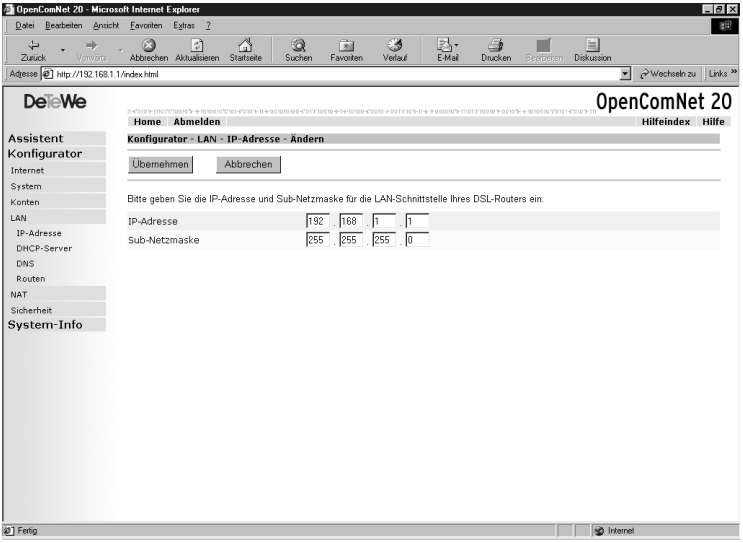


IP-Adresse	Die IP-Adresse des Routers.
DHCP Server	DHCP-Netz konfigurieren bzw. ein- und ausschalten.
DNS	Einstellungen für DNS (Domain Name Service).
Routen	Konfigurieren von statischen Routern.

IP-Adresse



Sie sehen jetzt die aktuellen Einstellungen. Wenn Sie Änderungen haben, klicken Sie auf **Ändern**.



Tragen Sie zunächst den richtigen Wert für Ihre Subnetzmaske ein. Hierdurch wird die Größe des lokalen Netzwerkes (LAN) definiert, das vom OpenComNet 20 verwaltet werden soll.

Ein **Klasse A** Netzwerk
umfasst bis zu 16.777.214 Rechner und benötigt die Netzwerkmaske: 255.0.0.0

Ein **Klasse B** Netzwerk
umfasst bis zu 65.534 Rechner und benötigt die Netzwerkmaske: 255.255.0.0

Ein **Klasse C** Netzwerk
umfasst bis zu 254 Rechner und benötigt die Netzwerkmaske: 255.255.255.0 (dieser Wert ist ab Werk voreingestellt).

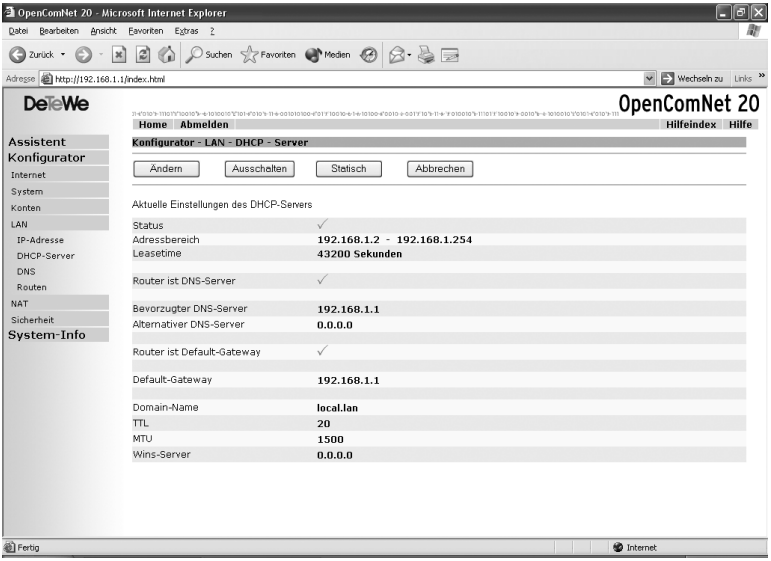
Da IP-Adressen weltweit sehr knapp geworden sind, erhält Ihr OpenComNet 20 vom Provider (in der Regel) immer nur leihweise eine WAN-IP-Adresse zugeteilt, die nur für die Dauer einer einzigen Interneteinwahl gültig ist.
OpenComNet 20 übersetzt diese Adresse mit Hilfe von NAT/PAT in lokale Netzwerkadressen, die aus Sicherheitsgründen einem Adressbereich entnommen werden, der im Internet nicht gültig ist.
Diese Adressbereiche sind wie folgt definiert:

Netzwerkklasse	von	bis
A	10.0.0.1	10.255.25.254
B	172.16.0.1	172.31.255.254
C	192.168.0.1	192.168.255.254

Wählen Sie die LAN-IP-Adresse Ihres OpenComNet 20 entsprechend der Netzwerkklasse aus den oben genannten Bereichen aus.

Klicken Sie danach auf **Übernehmen**.

DHCP Server

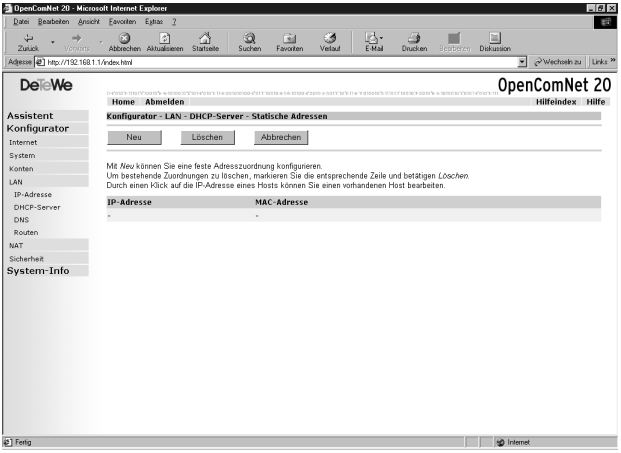


Sie sehen jetzt die aktuellen Einstellungen.
Klicken Sie **Einschalten/Ausschalten** wenn Sie den DHCP-Server aktivieren oder deaktivieren wollen.

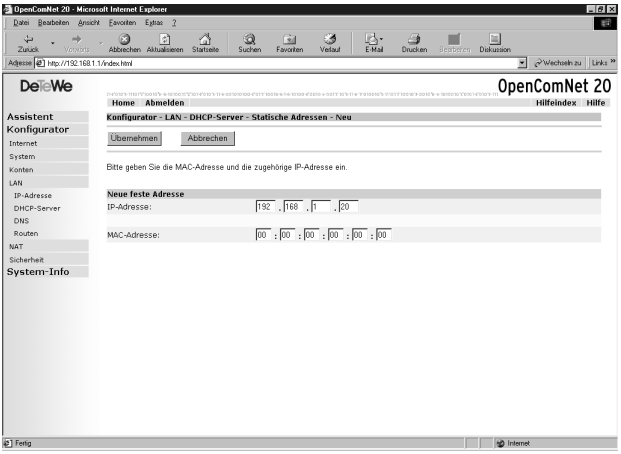
Hinweis

Bei deaktiviertem DHCP-Server müssen Sie alle IP-Adressen für Ihre Client-Rechner im lokalen Netzwerk (LAN) statisch (manuell) eingeben.

Klicken Sie auf **Statisch**, wenn Sie unabhängig vom DHCP-Server einzelnen Rechnern im lokalen Netzwerk eine feste IP-Adresse geben wollen. Dies ist z. B. dann sinnvoll, wenn diese Rechner Server-Dienste übernehmen sollen.



Klicken Sie auf **Neu**.

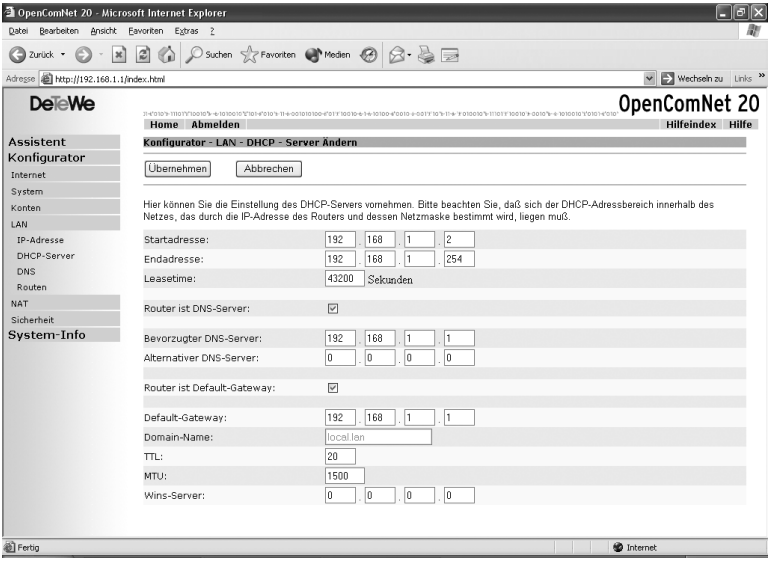


Geben Sie die IP-Adresse ein, die Sie fest vergeben wollen.
Wählen Sie diese Adresse aus dem hierfür vorgesehenen Bereich Ihrer Netzwerkklasse aus:

Netzwerkklasse	von	bis
A	10.0.0.1	10.255.25.254
B	172.16.0.1	172.31.255.254
C	192.168.0.1	192.168.255.254

Geben Sie die dazugehörige MAC-Adresse ein. Diese Adresse ist auf der Hardware z. B. der Netzwerkkarte des Rechners aufgedruckt.
Klicken Sie auf **Übernehmen**.

Wenn Sie bei den übrigen Eintragungen Änderungen vornehmen möchten, klicken Sie auf **Ändern**.



- **DHCP-Server**
  Wenn Sie den DHCP-Server aktiviert haben, vergibt er alle in Ihrem lokalen Netzwerk benötigten IP-Adressen automatisch aus einem von Ihnen definierten Adressbereich.
  Sie müssen diesen Bereich durch eine Start- und eine Endadresse festlegen. Abhängig von der Netzwerkklasse Ihres lokalen Netzwerks stehen Ihnen hierfür folgende Adressbereiche zur Verfügung:

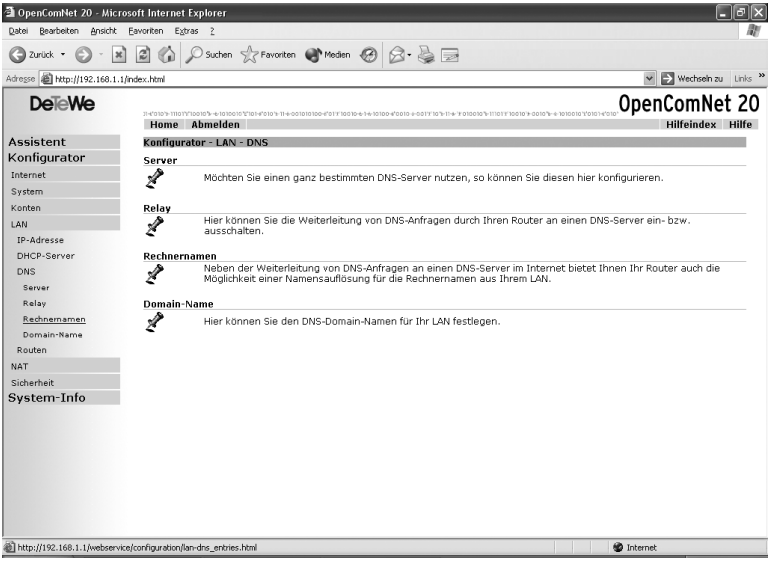
Netzwerkklasse	Max. Rechneranzahl	von	bis
A	16.777.214	10.0.0.1	10.255.25.254
B	65.534	172.16.0.1	172.31.255.254
C	254	192.168.0.1	192.168.255.254

- **Leasetime**
  Die IP-Adressen vom DHCP-Server sind nur für die Dauer der „Leasetime“ gültig, danach verfallen sie und werden ggf. automatisch neu vergeben. Die Neuvergabe erfolgt normalerweise unterbrechungsfrei. Diese regelmäßige Neuvergabe hat zwei Vorteile: zum Einen werden IP-Konflikte - sofern sie auftreten - hierdurch automatisch gelöst; zum Anderen kann man hierdurch z. B. in einem Klasse C Netz unter der Prämisse, dass nicht alle Rechner gleichzeitig „Online“ sind, auch mehr als 254 Rechner (z. B. 300) betreiben. Wir empfehlen eine Leasetime von 1 h (= 3.600 Sekunden).

- **Router ist DNS-Server**
  Der DNS (Domain Name Server) setzt Domain-Namen in IP-Adressen um. Aktivieren Sie diese Funktion, sofern Sie nicht einen anderen DNS-Server im lokalen Netzwerk nutzen wollen.
- **Bevorzugter DNS-Server**
  Tragen Sie hier die LAN-IP-Adresse Ihres OpenComNet 20 ein.
- **Alternativer DNS-Server**
  Hier können Sie die IP-Adresse eines Ausweich DNS-Servers im LAN eintragen.
- **Default-Gateway**
  Ist zu aktivieren, wenn OpenComNet 20 Ihren Internetzugang bereitstellen soll. Tragen Sie in diesem Fall die LAN-IP-Adresse Ihres OpenComNet 20 ein. Soll ein anderer Router den Internetzugang bereitstellen, ist dessen IP-Adresse hier einzutragen.
- **Domain-Name**
  Name des lokalen Netzwerks (nur Anzeige). Änderungen sind nur über die Eingabemaske „Konfigurator/LAN/DNS/Domain Name“ zulässig.
- **TTL**
  (Time to live) Die maximale Anzahl von „hops“ (Routersprüngen), die ein Datenpaket ausführen kann, bevor es verworfen wird. Der voreingestellte Wert „20“ ist bei der derzeitigen Internetgröße der zu empfehlende Wert.
- **MTU** (Maximum Transmission Unit)
  Mit diesem Wert wird die Größe der Datenpakete festgelegt und damit die Datenübertragungsgeschwindigkeit beeinflusst. Sinnvolle Paketgrößen liegen zwischen 576 und 1492. Der voreingestellte Wert von 1500 ist in der Regel das Optimum. In Einzelfällen kann es vorkommen dass Netzwerkkomponenten diesen hohen MTU-Wert nicht problemlos verarbeiten können. In diesem Falle ist der Wert experimentell zu reduzieren.
- **Wins-Server**
  Das Auffinden von Windows-Ressourcen kann erheblich beschleunigt werden, wenn ein Wins-Server im LAN betrieben wird. Dies gilt insbesondere für NT und ältere Betriebssysteme. Außerdem wird die Netzlast, die bei der Verbreitung von Windows-Rechnernamen entsteht, hierdurch erheblich reduziert. Wenn Sie einen Wins-Server im LAN betreiben, tragen Sie bitte hier dessen IP-Adresse ein.

Klicken Sie anschließend auf **Übernehmen**.

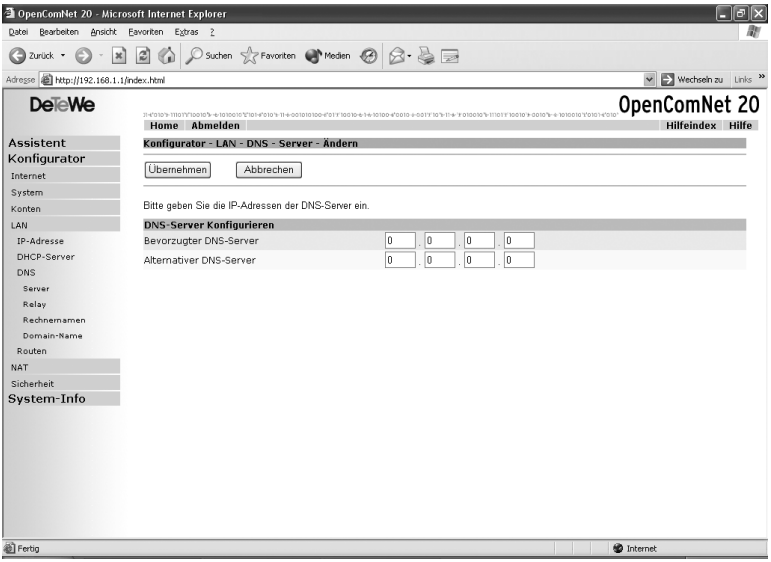
DNS



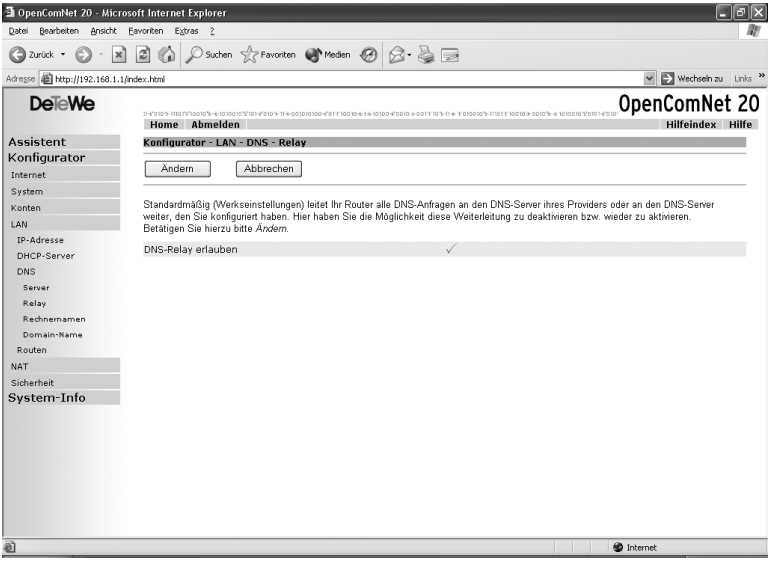
Server	Konfiguration eines alternativen DNS-Servers im Internet.
Relay	Ein- bzw. ausschalten der Weiterleitung von DNS-Anfragen.
Rechnernamen	Neben der Weiterleitung von DNS-Anfragen an einen DNS-Server im Internet bietet Ihnen Ihr Router auch die Möglichkeit einer Namensauflösung für die Rechnernamen aus Ihrem LAN.
Domain-Name	Name des lokalen Netzwerks.

Sie können alternativ zu dem von Ihrem Provider zur Verfügung gestellten DNS-Server einen bevorzugten DNS-Server im Internet definieren, den Sie bei der Einwahl ins Internet benutzen möchten.

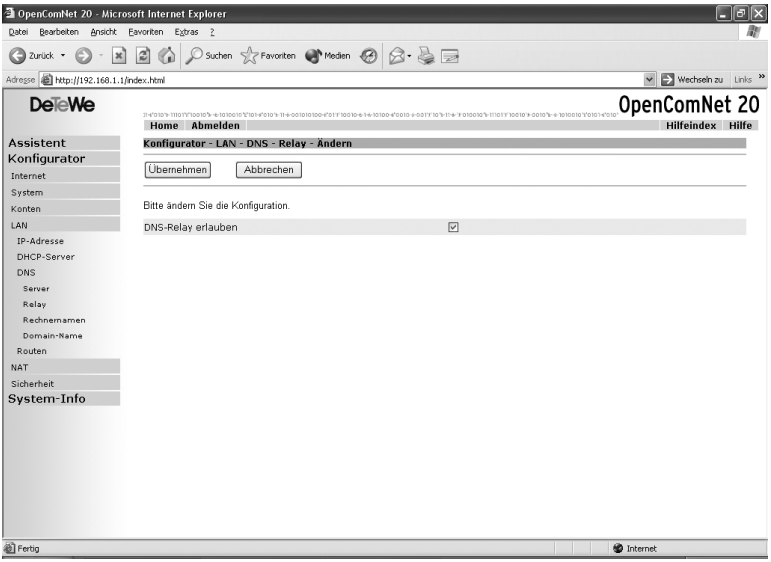
Klicken Sie auf **Ändern** wenn Sie vorzugsweise einen bestimmten DNS-Server nutzen möchten.



Tragen Sie die IP-Adressen in die entsprechenden Felder ein und klicken Sie danach auf **Übernehmen**.



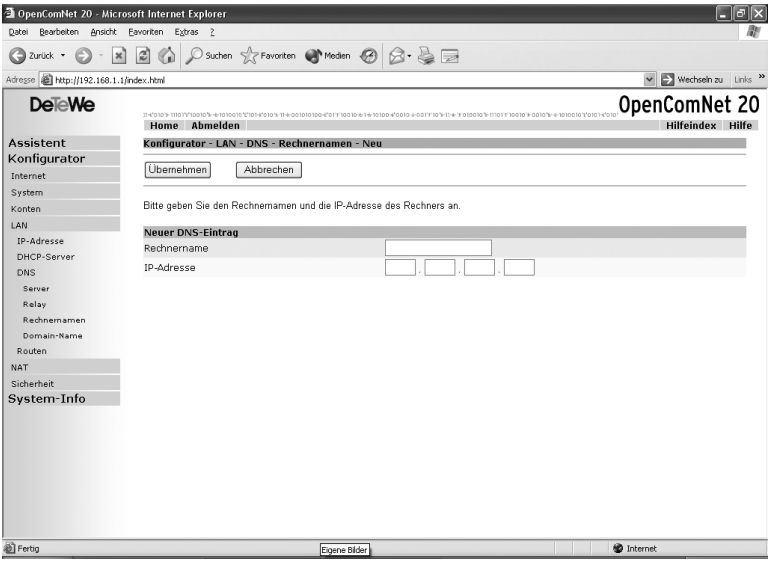
Klicken Sie auf **Ändern** wenn Sie die Weiterleitung Ihrer DNS-Anfragen (DNS-Relay) an den DNS-Server Ihres Providers oder an einen von Ihnen selbst konfigurierten DNS-Server im Internet deaktivieren bzw. wieder aktivieren möchten.



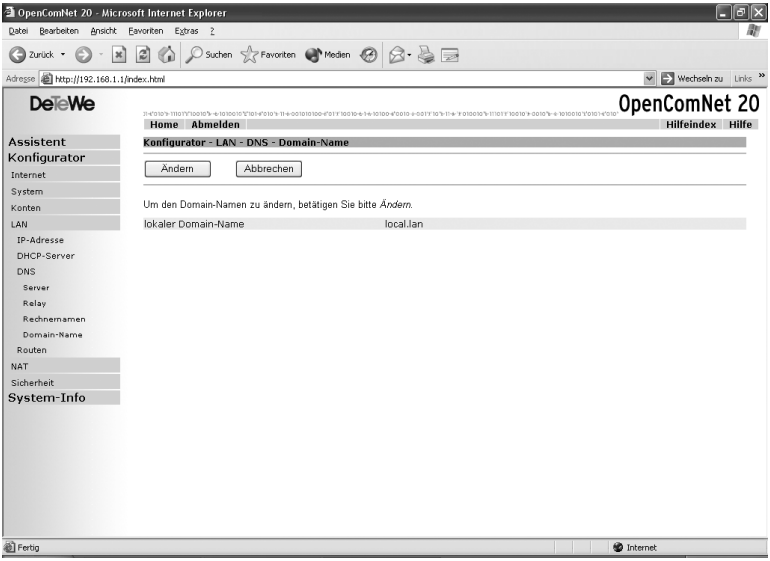
Markieren Sie die Checkbox entsprechend und klicken Sie danach auf **Übernehmen**.

Für Rechner, die ihre IP-Adresse automatisch vom OpenComNet 20 beziehen, wird automatisch eine Eintrag angelegt. Betreiben Sie in Ihrem LAN Rechner, die eine feste IP-Adresse besitzen, legen Sie bitte für jeden dieser Rechner selbst einen eigenen Eintrag an.

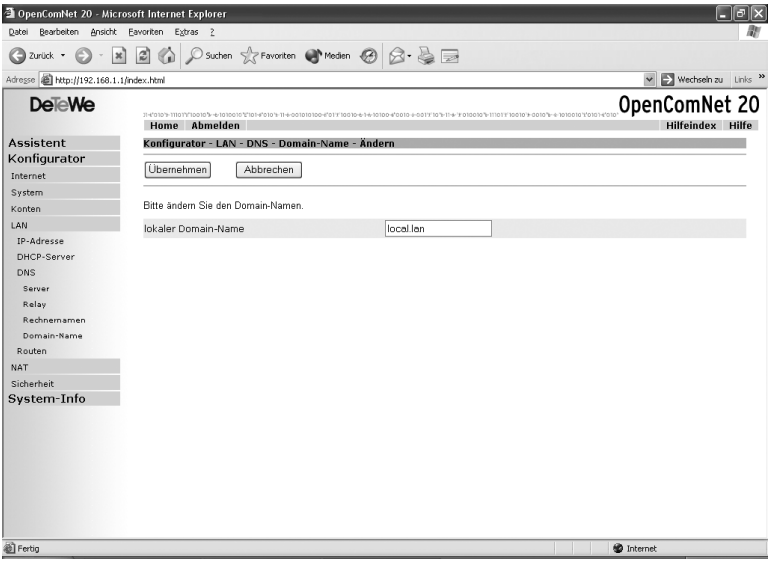
Klicken Sie auf **Neu**, geben Sie zur Identifizierug einen Namen für den Rechner und die feste IP-Adresse ein und klicken Sie auf **Übernehmen**.



Sie können den Domain-Namen Ihres LAN verändern.



Klicken Sie auf **Ändern**, geben Sie den neuen Domain-Namen ein und klicken Sie auf **Übernehmen**.



Hinweis

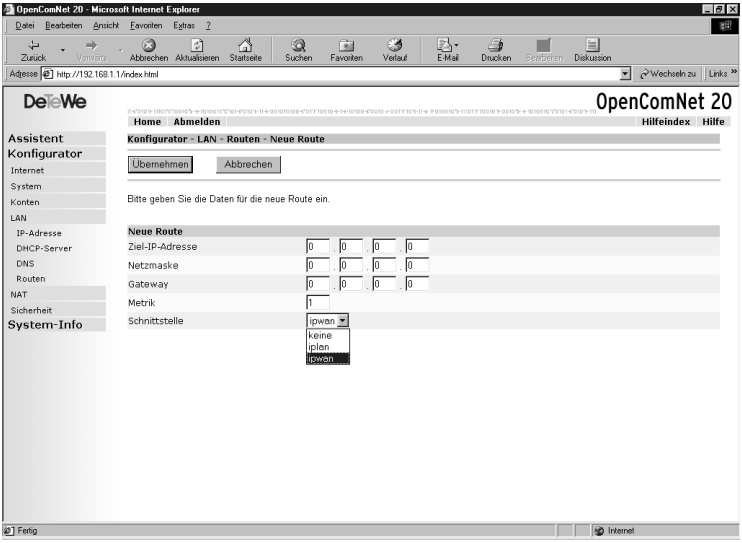
Wenn Sie den Domain-Namen ändern, beachten Sie bitte, dass sich der Zugang zum Konfigurator (sofern Sie nicht die IP-Adresse des OpenComNet 20 benutzen) ebenfalls ändert (s. Seite 23).

Routen

In der Liste erscheinen die zur Zeit bestehenden Routen.

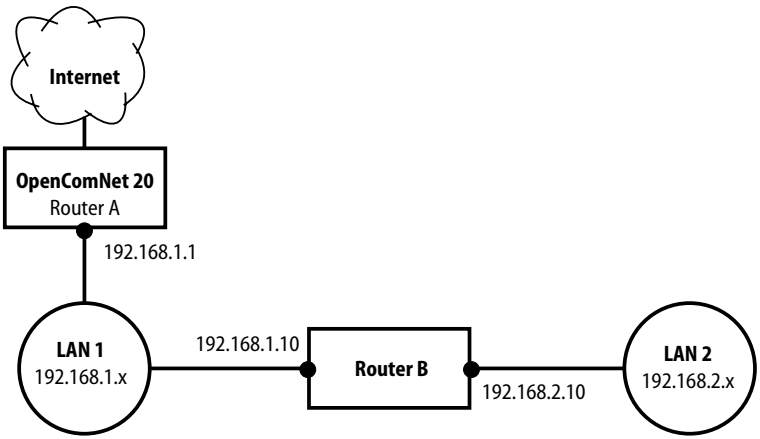
- Neu - legt einen neuen Eintrag an.
- Nach Anklicken der Zieladresse kann eine bestehende Route bearbeitet werden.
- Löschen - vorher einen Eintrag markieren, dann auf Löschen klicken.

Klicken Sie auf **Neu**.



Routen werden benötigt, um Datenpakete gezielt von einem Netzwerk in ein anderes zu schicken.

Hierzu ein Beispiel:



In diesem Beispiel ist für die WAN-Seite von Router A (OpenComNet 20) keine IP-Adresse angegeben, weil diese vom Internetprovider üblicherweise immer nur für die Dauer einer Internetsitzung

vergeben wird. Die LAN-IP-Adresse von Router A ist 192.168.1.1. Router B hat zwei IP-Adressen, 192.168.1.10 für LAN 1 und 192.168.2.10 für LAN 2.
Um Datenpakete vom OpenComNet 20 ins LAN 2 schicken zu können, muss folgende Route angelegt werden:

Ziel-IP-Adresse	**Netzmaske**	**Gateway**	**Metrik**	**Schnittstelle**
192.168.2.0	255.255.255.0	192.168.1.10	1	iplan

Ziel IP-Adresse: 192.168.2.0 (Durch die Null wird der Adressenbereich von 192.168.2.1 bis 192.168.2.254 gekennzeichnet)

Netzmaske: 255.255.255.0 (Weil LAN 2 ein Klasse C Netzwerk ist)

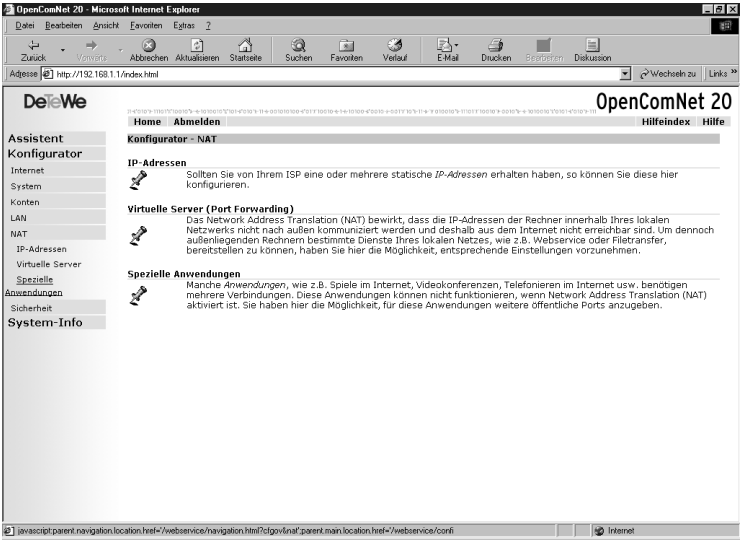
Gateway: 192.168.1.10 (Weil diese Adresse von Router B das Gateway (Eingangstor) zum LAN 2 bildet)

Metrik: 1 Das Internet/Intranet ist redundant aufgebaut d. h., es gibt häufig mehrere Routen um von A nach B zu kommen. Wenn Sie daher alternative Routen programmieren, müssen Sie über die Metrikziffer festlegen (meist unter Kostengesichtspunkten), welche Route Sie bevorzugt nutzen wollen. Die Route mit der niedrigsten Ziffer wird immer zuerst probiert. Ist diese Route überlastet oder unterbrochen, wird automatisch die Route mit der nächst höheren Metrik gewählt.

Schnittstelle: iplan (Weil das Ziel in diesem Beispiel auf der LAN-Seite des Routers liegt.) Befände sich das Ziel im Internet, würde man „ipwan“ auswählen. Wenn „keine“ aktiviert wird, sucht OpenComNet 20 automatisch die richtige Schnittstelle.

Tragen Sie die Angaben in die entsprechenden Felder ein und klicken Sie danach auf **Übernehmen**.

NAT


OpenComNet 20 - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Bearbeiten Diskussion
Adresse http://192.168.1.1/index.html
Wechseln zu Links
DeTeWe
OpenComNet 20
Home Abmelden
Hilfeindex Hilfe
Assistent
Konfigurator
Internet
System
Konten
LAN
NAT
IP-Adressen
Virtuelle Server
Spezielle Anwendungen
Sicherheit
System-Info
Konfigurator - NAT
IP-Adressen
Sollten Sie von Ihrem ISP eine oder mehrere statische IP-Adressen erhalten haben, so können Sie diese hier konfigurieren.
Virtuelle Server (Port Forwarding)
Das Network Address Translation (NAT) bewirkt, dass die IP-Adressen der Rechner innerhalb Ihres lokalen Netzwerks nicht nach außen kommuniziert werden und deshalb aus dem Internet nicht erreichbar sind. Um dennoch außenliegenden Rechnern bestimmte Dienste Ihres lokalen Netzes, wie z.B. Webservice oder Filetransfer, bereitstellen zu können, haben Sie hier die Möglichkeit, entsprechende Einstellungen vorzunehmen.
Spezielle Anwendungen
Manche Anwendungen, wie z.B. Spiele im Internet, Videokonferenzen, Telefonieren im Internet usw. benötigen mehrere Verbindungen. Diese Anwendungen können nicht funktionieren, wenn Network Address Translation (NAT) aktiviert ist. Sie haben hier die Möglichkeit, für diese Anwendungen weitere öffentliche Ports anzugeben.
javascript:parent.navigation.location.href='/webservice/navigation.html?cfgov&nat';parent.main.location.href='/webservice/confi
Internet

IP-Adressen — Feste IP-Adressen (wurden Ihnen von Ihrem Internetprovider mitgeteilt).

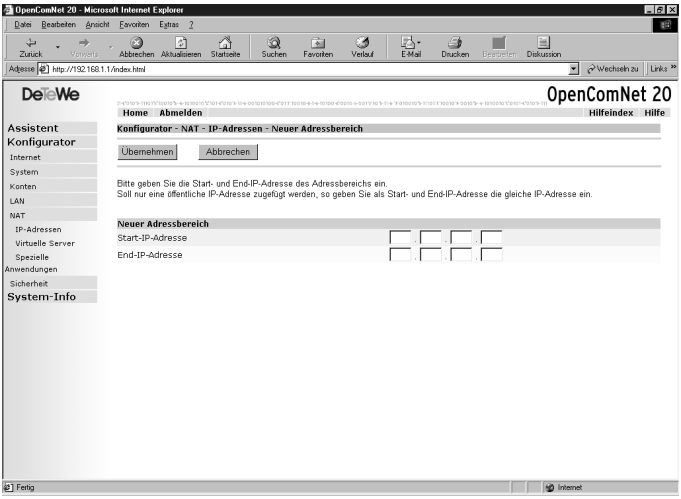
Virtueller Server (Port Forwarding) — Dieses Merkmal, auch bekannt unter **Port Forwarding**, erlaubt es Ihnen, Server Ihres Netzwerkes anderen Internetbenutzern zugänglich zu machen. Normalerweise könnte ein Server Ihres Netzwerkes aus dem Internet nicht erreicht werden, denn:

- Ihre Netzwerkserver haben keine im Internet gültige IP-Adresse.
- Versuche, einen Server im LAN aus dem Internet zu erreichen, werden von der Firewall blockiert.

Spezielle Anwendung — Manche Anwendungen benötigen nur dann Ports, wenn sie gerade aktiv genutzt werden (z. B. IP-Telefonie oder Videokonferenzen). Diese können hier konfiguriert werden.

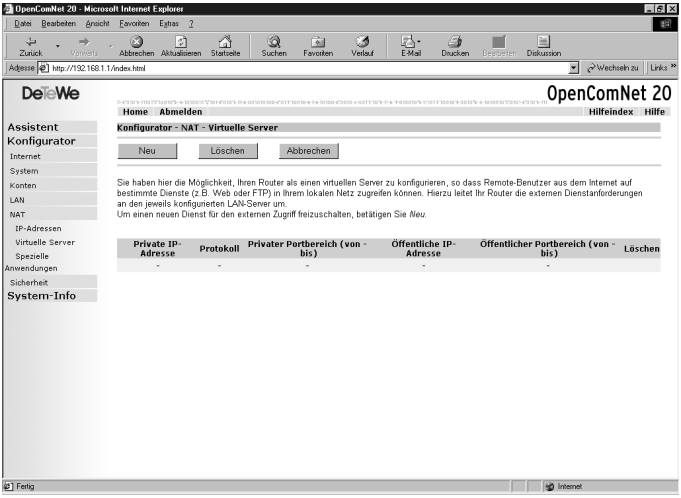
- IP-Adressen

Haben Sie bereits feste IP-Adressen von Ihrem Serviceprovider erhalten, finden Sie sie in der Liste. Mit **Löschen** können Sie einen markierten Eintrag löschen. Wollen Sie einen neuen Bereich in die Liste aufnehmen, klicken Sie auf **Neu**.

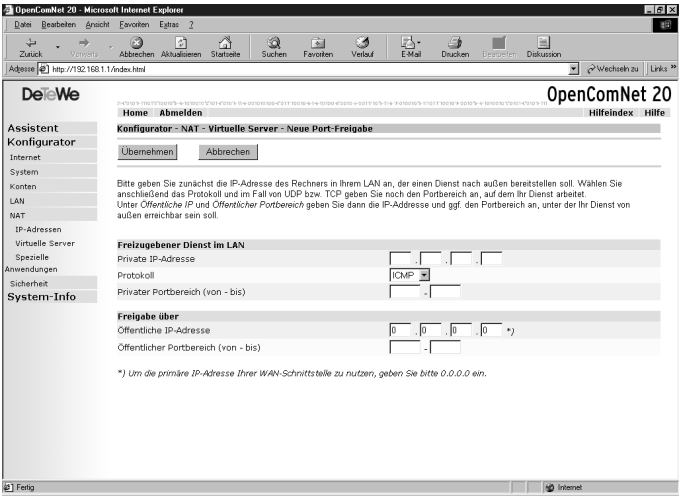


Tragen Sie unter Start IP-Adresse und End IP-Adresse die Werte ein, die Ihnen Ihr Serviceprovider mitgeteilt hat. Danach klicken Sie auf **Übernehmen**.

- Virtueller Server



In der Liste sind nur Einträge vorhanden, wenn der Router bereits als virtueller Server betrieben wird. Mit **Löschen** entfernen Sie einen markierten Eintrag und mit **Neu** legen Sie einen neuen virtuellen Server an. Klicken Sie auf **Neu**.


OpenComNet 20 - Microsoft Internet Explorer
DeTeWe
OpenComNet 20
Home Abmelden
Hilfeindex Hilfe
Assistent
Konfigurator
Konfigurator - NAT - Virtuelle Server - Neue Port-Freigabe
Übernehmen
Abbrechen
Bitte geben Sie zunächst die IP-Adresse des Rechners in Ihrem LAN an, der einen Dienst nach außen bereitstellen soll. Wählen Sie anschließend das Protokoll und im Fall von UDP bzw. TCP geben Sie noch den Portbereich an, auf dem Ihr Dienst arbeitet.
Unter Öffentliche IP und Öffentlicher Portbereich geben Sie dann die IP-Addresse und ggf. den Portbereich an, unter der Ihr Dienst von außen erreichbar sein soll.
Freizugegebener Dienst im LAN
Private IP-Adresse
Protokoll
ICMP
Privater Portbereich (von - bis)
Freigabe über
Öffentliche IP-Adresse
Öffentlicher Portbereich (von - bis)
*) Um die primäre IP-Adresse Ihrer WAN-Schnittstelle zu nutzen, geben Sie bitte 0.0.0.0 ein.

Virtuelle Server benötigt man, um Dienste, die firewallbedingt eigentlich nur im LAN zur Verfügung stehen, auch vom Internet her zugänglich zu machen. Da die Rechner im LAN keine im Internet gültigen IP-Adressen haben, müssen diese Adressen hierfür in die jeweils vom Provider zugeteilte IP-Adressen der WAN-Schnittstelle umgesetzt werden.

Protokolle

Das **TCP-Protokoll** ermöglicht einen quittierten Datenaustausch zwischen zwei Endpunkten. Es sorgt dafür, dass Datenpakete nicht verloren gehen, im Fehlerfall wiederholt werden und in der Reihenfolge beim Empfänger eintreffen, in der sie der Absender geschickt hat. Um diese Aufgaben zu erfüllen, wird neben den eigentlichen Nutzdaten eine größere Anzahl zusätzlicher Informationen übermittelt.

Das **UDP-Protokoll** ermöglicht einen unquittierte Datenaustausch zwischen zwei Endpunkten. Beim Absenden eines UDP-Pakets kann der Sender also nicht sicher davon ausgehen, dass das Paket auch beim Empfänger ankommt. Dafür benötigt dieses Protokoll nur sehr wenige Zusatzinformationen, was in einem störungsfrei funktionierenden Netzwerk, wie z. B. einem LAN, zu einem besseren Datendurchsatz führt.

Das **ICMP-Protokoll** dient zur Übermittlung von Informationen über das Netzwerk selbst, wie z. B. die Verfügbarkeit bestimmter Pfade innerhalb des Netzwerks, ob bestimmte Rechner erreichbar sind usw. So sendet beispielsweise das für Diagnosezwecke oft eingesetzte „ping" ein ICMP-Paket an den Zielrechner mit der Aufforderung, dieses Paket unverändert zurückzusenden (ICMP echo request).

Neben diesen existiert noch eine Fülle anderer Protokolle für die verschiedensten Aufgaben (Dienste). Sie tauschen ihre Protokolldatenpakete in den Endpunkten über die beiden Transportprotokolle TCP und UDP aus. Die überwiegende Anzahl von Diensten im Internet werden über TCP transportiert:

- Das **HTTP-Protokoll (WWW)** ermöglicht die Kommunikation von Web-Browsern (InternetExplorer, Mozilla, Netscape, Opera, ...) mit WEB-Servern im Netz und damit das Surfen im Internet oder Intranet.
- Das **FTP-Protokoll** (Dateitransfer) ermöglicht den Austausch von Dateien im Netz. Lokale FTP-Programme (WS-FTP, ...) kommunizieren hierfür mit File(FTP)-Servern im Netz.
- Die **SMTP/POP3/IMAP-Protokolle** ermöglichen den Austausch von elektronischen Nachrichten (Email) im Netz. Lokale Mail-Programme (oft integriert in WEB-Browser- oder Office-Produkten) kommunizieren hierfür mit Mail-Servern von Service-Providern.
- Das **DNS-Protokoll** ermöglicht lokal und weltweit das Auflösen von logischen Namen (z.B. t-online.de) im Netz, in die in allen Netzelementen verwendeten IP-Adressen (194.25.134.146). Benutzt ein Netzelement einen logischen Rechnernamen, so wird ein DNS-Request an den nächsten eingerichteten DNS-Server gestellt, der versucht diesen Namen aufzulösen oder weiterzuleiten.

Einfachere Dienste werden im Netz jedoch über UDP transportiert. Oft sind es auch einseitig gerichtete - oder Broadcast-Verbindungen:

- Das **DHCP-Protokoll** ermöglicht die eindeutige Vergabe von Netzwerk (IP-Adressen) in lokalen Netzen, die der DHCP-Server den Rechnern in lokalen Netzen zuweist.
- Das **TFTP-Protokoll** ermöglicht einen einfachen Austausch von Dateien. Es wird oft zum Download binär-Dateien zum Software-Update in den Netzelementen verwendet.
- Das **SNTP-Protokoll** ermöglicht die Datum- und Uhrzeitsynchronisation von Systemen mit Time-Servern im Netz.
- Das **SNMP-Protokoll** ermöglicht die Steuerung und Administration von Systemen im Netz.
- **Voice over IP (VoIP)** verwendet ebenfalls einige Protokolle über UDP. Dies ist in dem hohen Ressourcenbedarf begründet, die die Telefonie über IP erfordert und die Sprachdaten einen nicht so hohen Sicherungsbedarf haben.

Nähere Details oder weitere TCP- und UDP-Protokolle sind hier nicht weiter erwähnt. Es wird auf die einschlägige Literatur verwiesen.

Ports
Ein einziger Rechner kann gleichzeitig mehrere Verbindungen aufbauen und auch mehrere Dienste für andere Rechner zur Verfügung stellen. Zur Unterscheidung dieser parallel laufenden Verbindungen werden die so genannten Ports verwendet, von denen es für TCP und UDP jeweils 65535 gibt. Aufgrund einer allgemeinen Vereinbarung bieten Server ihre Dienste üblicherweise auf den Ports 1 .. 1023 für die kommenden Verbindungen an. Den oben beschriebenen Protokollen sind jeweils feste Ports aus diesem Bereich zugeteilt. Von den Servern abgehende Verbindungen werden normalerweise von Ports ab 1024 aufgebaut. Diese Festlegung ist aber nur eine Konvention und nicht technisch bedingt. Es kann durchaus sinnvoll sein, Dienste auf „hohen" Ports (Ports über 1023) anzubieten. Da traditionell auf den niedrigen Ports auch potentiell unsichere oder sensible Dienste angeboten werden, sind die meisten Firewalls so konfiguriert, dass auf diese Ports nur sehr eingeschränkt zugegriffen werden darf. Auch sind üblicherweise besondere Rechte (root- bzw. Administrator-Rechte) erforderlich, um Dienste an Ports unter 1024 zu binden.

Bevor Sie die Maske für virtuelle Server ausfüllen können, müssen Sie sicherstellen, dass der oder die Rechner, die Serverdienste übernehmen sollen, feste interne IP-Adressen haben (siehe auch Seite 55ff).

Machen Sie jetzt in den Feldern die erforderlichen Angaben.

- Freizugebender Dienst im LAN
  Private IP - tragen Sie hier bitte die LAN-IP-Adresse Ihres Servers ein

  Protokoll - wählen Sie aus der Liste das gewünschte Protokoll aus.

  Privater Portbereich (von - bis) - geben Sie hier den Portbereich an, der für Ihren Serverdienst genutzt werden soll.

- Freigabe über
  Öffentliche IP - Sofern Sie von Ihrem Provider für jede Internetsitzung eine WAN-IP-Adresse dynamisch zugeteilt bekommen, brauchen Sie den voreingestellten Wert „0.0.0.0“ nicht zu verändern. Wenn Sie eine fixe WAN-IP-Adresse besitzen, tragen Sie sie bitte hier ein.

  Öffentlicher Portbereich (von - bis) - Für die meisten Anwendungen sind öffentlicher- und privater Portbereich identisch. Gelegentlich kann es jedoch einmal vorkommen, dass Sie im privaten Bereich Ihre Portbelegung anders gestalten möchten, als das im öffentlichen Bereich üblich ist. Tragen Sie hier den Portbereich ein den Sie auf der WAN-Seite benutzen wollen.

Filesharing
Zu den beliebtesten Applikationen, die virtuelle Server benötigen, gehören die sog. Filesharing Programme. Hierbei handelt es sich um Anwendungen, mit deren Hilfe man im Internet z. B. Musikstücke oder Spielfilme tauschen kann. Um diese Tauschvorgänge möglichst schnell abzuwickeln, werden hierfür vom OpenComNet 20 teilweise viele 100 Internetverbindungen gleichzeitig aufgebaut.

Hinweis

Achten Sie darauf, dass Sie nur solche Dateien zum Tausch anbieten, für die Sie auch die Urheberrechte besitzen.

Im Folgenden finden Sie eine kurze Übersicht über die gebräuchlichsten Filesharing Programme und die hierfür benötigten Protokolle und Portbereiche. Diese ist jedoch nur als „Momentaufnahme“ zu betrachten. Die aktuellen Einstellungen entnehmen Sie bitte den jeweiligen Handbüchern.

- FastTrack - Kazaa/KazaaLite/Grokster/iMesh Konfiguration
  FastTrack ist das beliebteste Peer to Peer-Netzwerk und Applikationen wie Kazaa, KazaaLite, Grokster und iMesh benutzen den Standardport 1214. Dieser Port kann in den Optionen der Applikation aber beliebig verändert werden. Im Router muss der Port sowohl gehend als auch kommend für TCP und UDP frei geschaltet werden.

- EDonkey/eMule Konfiguration
  EDonkey und eMule verwenden die Ports 4662 TCP und 4672 UDP, die in der Applikation geändert werden können. Um einen EDonkey/eMule-Client mit den Standardeinstellungen an dem Router betreiben zu können, sollten diese Ports in beiden Richtungen frei geschaltet werden.

- Gnutella - BearShare/Limewire/Morpheus/ToadNode Konfiguration
  Gnutella ist ein Open Source Protokoll und wird von über 50 Applikationen verwendet. Beliebte Peer to Peer-Applikationen sind BearShare, Limewire, Morpheus und ToadNode. Leider verwenden diese Peer to Peer-Applikationen unterschiedliche Ports, z. B.

  BearShare
  6346 TCP/UDP - Listening- und Server-Port, konfigurierbar

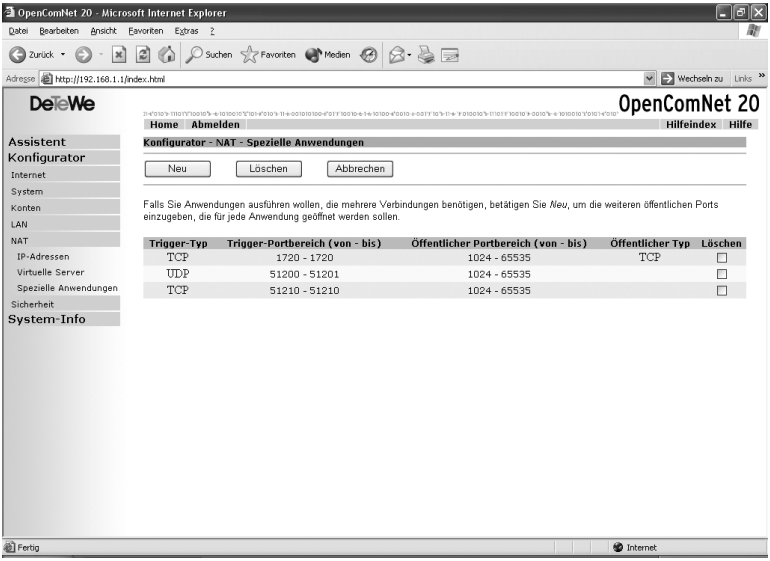
  Morpheus
  10897 TCP - konfigurierbar
  10898 TCP - Neonet-Port, konfigurierbar
  4662 TCP - EDonkey-Port

  Hier hilft nur ein Blick in die Online-Hilfe bzw. in die Einstellungen der Applikation und das anschließende Freischalten der entsprechenden Ports.

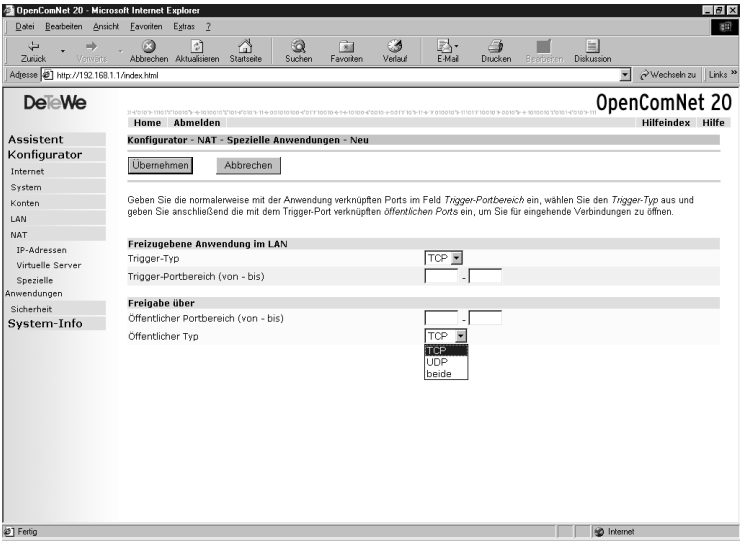
Online Spiele
Moderne Online Spiele fungieren häufig nicht nur als Client sondern auch als Server. Hierfür können für TCP und UDP bestimmte Ports über die Funktion „Virtueller Server“ so freigeschaltet werden, dass das ganze Internet auf sie zugreifen kann.

Sind Sie mit den Einstellungen fertig, klicken Sie auf **Übernehmen**.

- Spezielle Anwendungen



In der Liste sind nur Einträge vorhanden, wenn bereits Anwendungen konfiguriert wurden. Mit **Löschen** entfernen Sie einen markierten Eintrag und mit **Neu** legen Sie einen neuen virtuellen Server an. Klicken Sie auf **Neu**.



NAT - Spezielle Anwendungen/Trigger
Dies ist der eleganteste Weg, um Ports für eine Applikation, die Internet-Server-Funktionen beinhaltet, freizuschalten. Hierbei kann es sich z. B. um Anwendungen wie IP-Telefonie, Videokonferenzen oder auch moderne Online Spiele handeln
Da zunächst eine Verbindung zum Server/Host aufgebaut werden muss, bevor dieser Zugriff auf die konfigurierten Ports erhält, stehen diese nicht dem gesamten Internet offen.
Allerdings muss die Applikation das Freischalten triggern (auslösen), deswegen wird dieses dynamische Verfahren oft auch als „Trigger" bezeichnet.

TCP - Protokoll
Das TCP-Protokoll stellt einen quittierten Datenaustausch zwischen zwei Endpunkten her. Es sorgt dafür, dass Datenpakete nicht verloren gehen, im Fehlerfall wiederholt werden und in der Reihenfolge beim Empfänger eintreffen, in der sie der Absender geschickt hat. Um diese Aufgaben zu erfüllen, wird neben den eigentlichen Nutzdaten eine größere Anzahl zusätzlicher Informationen übermittelt.

UDP - Protokoll
Das UDP-Protokoll ermöglicht einen unquittierten Datenaustausch. Beim Absenden eines UDP-Pakets kann der Sender also nicht sicher davon ausgehen, dass das Paket auch beim Empfänger ankommt. Dafür benötigt dieses Protokoll nur sehr wenige Zusatzinformationen, was in einem störungsfrei funktionierenden Netzwerk, wie z. B. einem LAN zu einem besseren Datendurchsatz führt.

Konsultieren Sie das Handbuch Ihrer Applikation und machen Sie in den Feldern die erforderlichen Angaben.

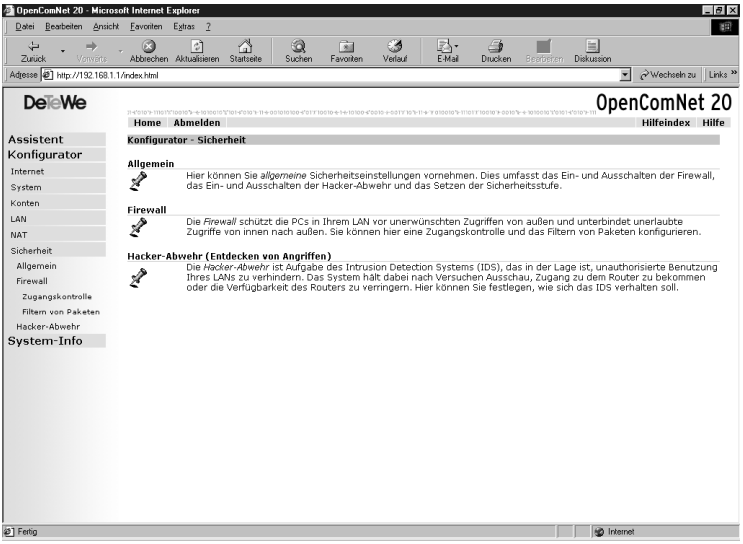
- Freizugebende Anwendung im LAN
  Trigger-Typ - wählen Sie das gewünschte Protokoll.
  Trigger-Portbereich (von - bis) - tragen Sie den für Ihre Applikation benötigten Portbereich ein.

- Freigabe über
  Öffentlicher Portbereich (von - bis) - Für die meisten Anwendungen sind öffentlicher- und privater Portbereich identisch. Gelegentlich kann es jedoch einmal vorkommen, dass Sie im privaten Bereich Ihre Portbelegung anders gestalten möchten, als das im öffentlichen Bereich üblich ist. Tragen Sie hier den Portbereich ein den Sie auf der WAN-Seite benutzen wollen.

  Öffentlicher Typ - wählen Sie zwischen TCP, UDP und „beide".

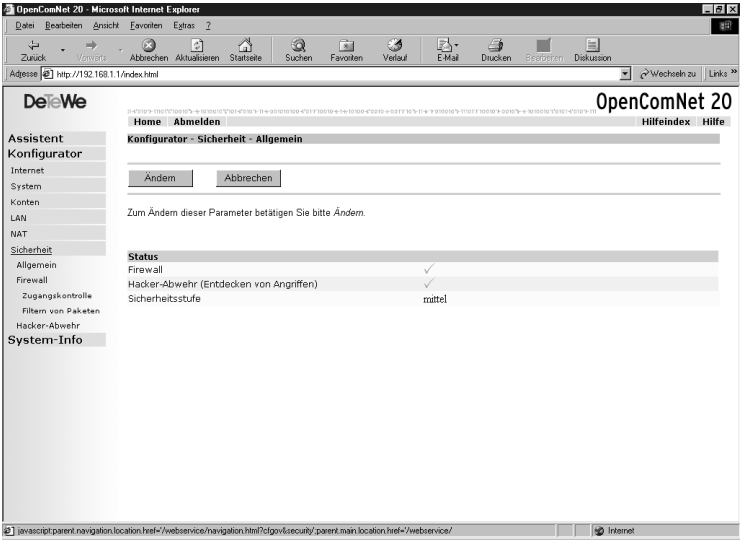
Sind Sie mit den Einstellungen fertig, klicken Sie auf **Übernehmen**.

Sicherheit

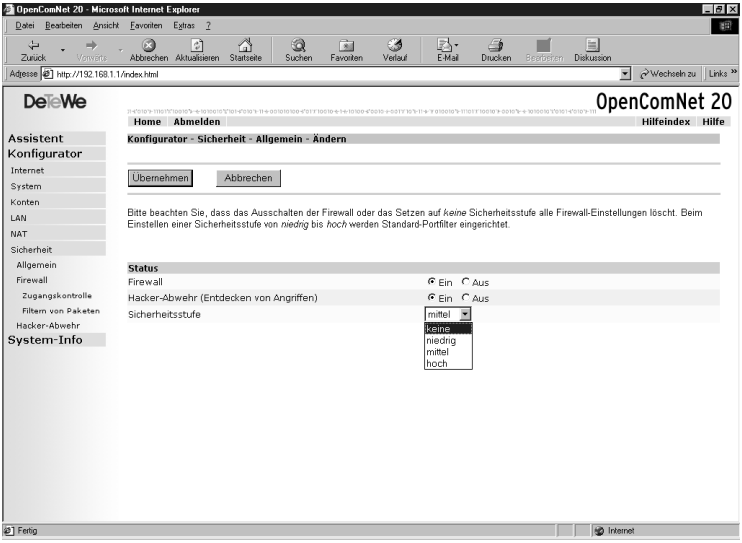

OpenComNet 20 - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Bearbeiten Diskussion
Adresse http://192.168.1.1/index.html
Wechseln zu Links
DeTeWe
OpenComNet 20
Home Abmelden
Hilfeindex Hilfe
Assistent
Konfigurator
Internet
System
Konten
LAN
NAT
Sicherheit
Allgemein
Firewall
Zugangskontrolle
Filtern von Paketen
Hacker-Abwehr
System-Info
Konfigurator - Sicherheit
Allgemein
Hier können Sie allgemeine Sicherheitseinstellungen vornehmen. Dies umfasst das Ein- und Ausschalten der Firewall, das Ein- und Ausschalten der Hacker-Abwehr und das Setzen der Sicherheitsstufe.
Firewall
Die Firewall schützt die PCs in Ihrem LAN vor unerwünschten Zugriffen von außen und unterbindet unerlaubte Zugriffe von innen nach außen. Sie können hier eine Zugangskontrolle und das Filtern von Paketen konfigurieren.
Hacker-Abwehr (Entdecken von Angriffen)
Die Hacker-Abwehr ist Aufgabe des Intrusion Detection Systems (IDS), das in der Lage ist, unauthorisierte Benutzung Ihres LANs zu verhindern. Das System hält dabei nach Versuchen Ausschau, Zugang zu dem Router zu bekommen oder die Verfügbarkeit des Routers zu verringern. Hier können Sie festlegen, wie sich das IDS verhalten soll.
Fertig
Internet

Allgemein	Hier legen Sie die grundlegenden Sicherheitsmaßnahmen fest.
Firewall	Zugangskontrollkriterien festlegen.
Entdecken von Angriffen (Hacker)	Verhindert die unauthorisierte Benutzung Ihres lokalen Netzwerkes. Sie legen hier die Abwehrmechanismen im Detail fest.

Allgemein



Sie sehen die aktuellen Einstellungen. Wollen Sie die Einstellungen korrigieren klicken Sie auf **Ändern.**



Aktivieren (Ein) bzw. Deaktivieren (Aus) Sie den Status indem Sie die Checkbox anklicken. Wählen Sie dann eine Sicherheitsstufe aus der Liste aus. Klicken Sie danach auf **Übernehmen**.

Sicherheitsoptionen

Die folgendeTabelle vermittelt eine Übersicht über die Dienste, die im Auslieferungszustand in Abhängigkeit von der gewählten Sicherheitsstufe freigeschaltet oder gesperrt sind. Hierbei wird für jeden Dienst angegeben, ob er in kommender- oder gehender Richtung nutzbar ist:

	Sicherheitsstufe: Niedrig			Mittel		Hoch	
Dienst	**Portbereich** (von/bis)	Richtung kommend	gehend	Richtung kommend	gehend	Richtung kommend	gehend
HTTP	80-80	gesperrt	offen	gesperrt	offen	gesperrt	offen
HTTPS	443-443	gesperrt	offen	gesperrt	offen	gesperrt	offen
T-Online-Homebanking	866-866	gesperrt	offen	gesperrt	offen	gesperrt	offen
IRC	113-113	offen	offen	offen	offen	offen	offen
IRC	6660-6669	gesperrt	offen	gesperrt	offen	gesperrt	offen
IRC	7000-7002	gesperrt	offen	gesperrt	offen	gesperrt	offen
Homebanking	3000-3000	gesperrt	offen	gesperrt	offen	gesperrt	offen
DNS (UDP)	53-53	offen	offen	gesperrt	offen	gesperrt	offen
DNS (TCP)	53-53	offen	offen	gesperrt	offen	gesperrt	offen
FTP	21-21	gesperrt	offen	gesperrt	offen	gesperrt	gesperrt
telnet	23-23	gesperrt	offen	gesperrt	offen	gesperrt	gesperrt
SMTP	25-25	gesperrt	offen	gesperrt	offen	gesperrt	offen
POP3	110-110	gesperrt	offen	gesperrt	offen	gesperrt	offen
NNTP	119-119	gesperrt	offen	gesperrt	offen	gesperrt	gesperrt
real Audio/Vid.	7070-7070	offen	offen	offen	offen	gesperrt	gesperrt
ICMP	–	gesperrt	offen	gesperrt	offen	gesperrt	offen
H.323	1720-1720	offen	offen	gesperrt	offen	gesperrt	gesperrt
T.120	1503-1503	offen	offen	gesperrt	offen	gesperrt	gesperrt
SSH	22-22	offen	offen	gesperrt	offen	gesperrt	gesperrt
NTP	123-123	offen	offen	offen	offen	offen	offen

Hinweise

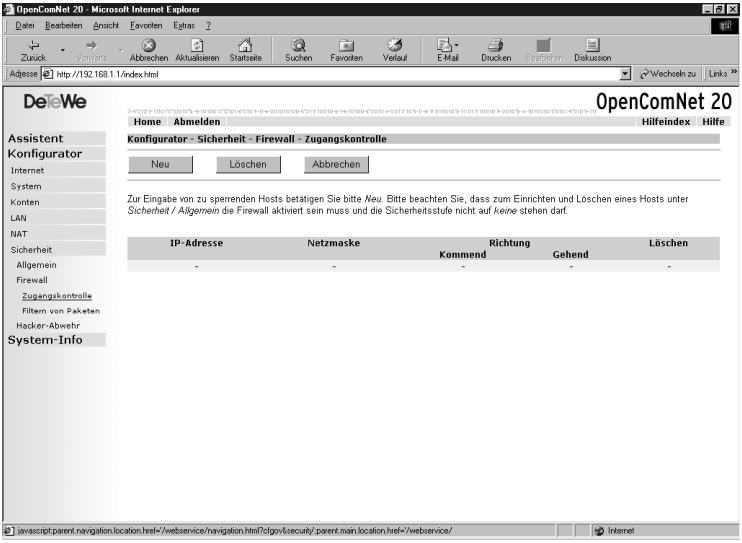
- Das Einstellen einer neuen Sicherheitsstufe löscht die Einstellungen der vorherigen Stufe inklusive der Paketfilter und richtet ggf. die Standardfilter ein.
- Die Sicherheitsstufe „keine“ ist eine leere Firewall-Konfiguration und erlaubt dem Benutzer, eigene Filterregeln zu definieren.

Firewall

Hinweis

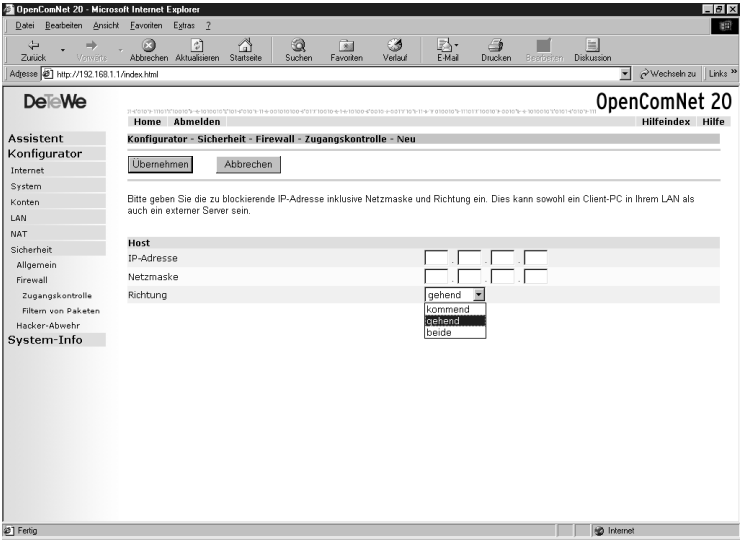
„Zugangskontrolle“ und „Filtern von Paketen“ lassen sich nur dann konfigurieren, wenn vorher die Firewall (siehe Seite 77) aktiviert worden ist und die Sicherheitsstufe nicht auf „keine“ steht.

- Zugangskontrolle



In der Liste finden Sie die bereits installierten Zugangsbeschränkungen. Sie können einen markierten Eintrag löschen, indem Sie auf **Löschen** klicken. Wollen Sie eine neue Beschränkung aufnehmen, klicken Sie auf **Neu**.

* Protokollnummern für IP beim Einrichten von Paketfiltern stehen in RFC1700 bzw. unter http://www.ietf.org/rfc/rfc1700.txt. Hier kann der Anwender ein Protokoll auswählen, wenn er weder TCP noch UDP einrichten möchte.



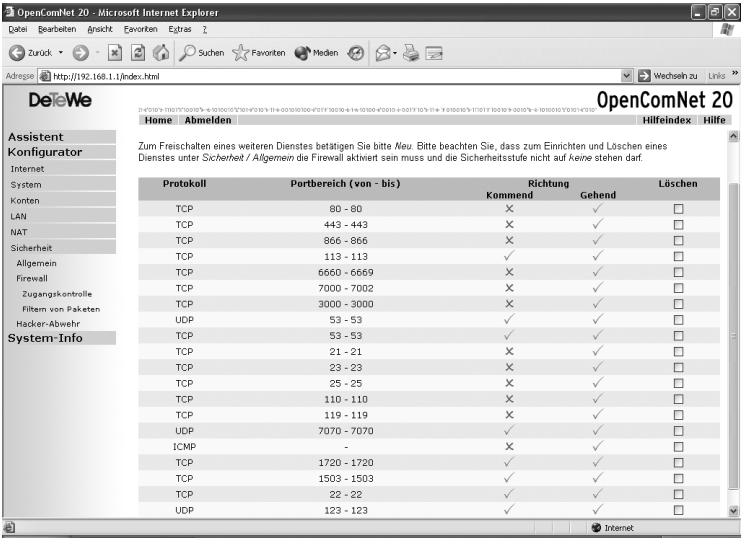
Machen Sie in den Feldern die erforderlichen Eintragungen.

Host

- IP-Adresse - IP-Adresse des zu blockierenden Servers.
- Netzmaske - Netzmaske Ihres LAN.
- Richtung - wählen Sie aus der Liste eine Vorgabe aus.

Haben Sie alle Einstellungen gemacht, klicken Sie auf **Übernehmen**.

- Filtern von Paketen

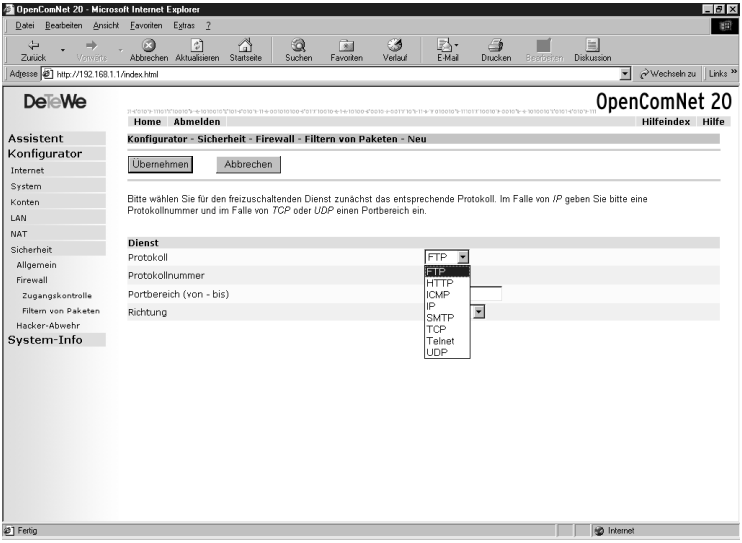


Sie sehen jetzt die aktuellen Einstellungen für die von Ihnen gewählte Sicherheitsstufe.

Hinweis

Alles, was hier nicht als freigeschaltet gelistet wird, ist gesperrt.
Sie können in der Spalte „Löschen“ Einträge auswählen und löschen, indem Sie auf **Löschen** klicken oder einen Dienst einrichten indem Sie auf **Neu** klicken.

Eine Auswahl von Einstellungen sortiert nach den Kategorien **Games**, **VPN**, **Audio/Video**, **Applications** und **Servers** finden Sie im Anhang.



Hier können für Dienste oder Netzwerkspiele gezielte Firewall-Freigaben konfiguriert werden. Bitte beachten Sie das jeweilige Handbuch. Für Spiele wird das TCP- oder UDP-Potokoll benötigt.

Machen Sie jetzt die entsprechenden Angaben in den Feldern.

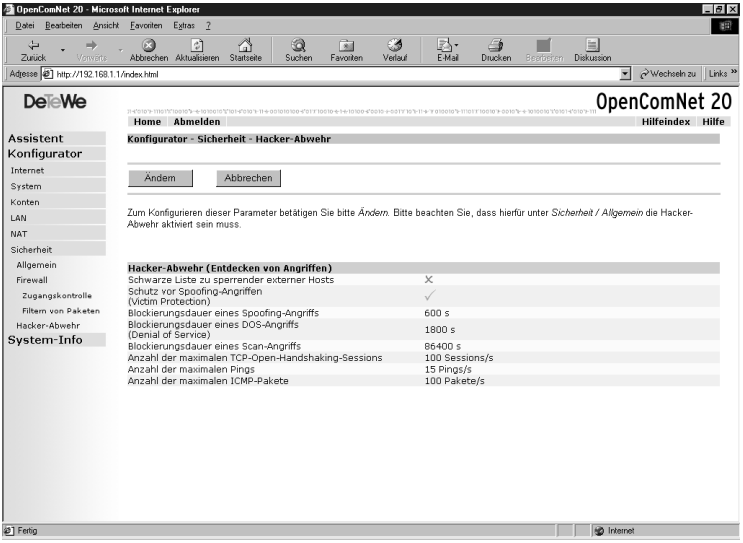
Dienst

- Protokoll - wählen Sie aus der Liste das von Ihrem Dienst benötigte Protokoll.
- Protokollnummer* - nur eintragen, wenn das IP-Protokoll gewählt wurde.
- Portbereich (von - bis) - nur eintragen, wenn das TCP- oder UDP-Protokoll gewählt wurde.
- Richtung - wählen Sie aus der Liste unter den Vorgaben.

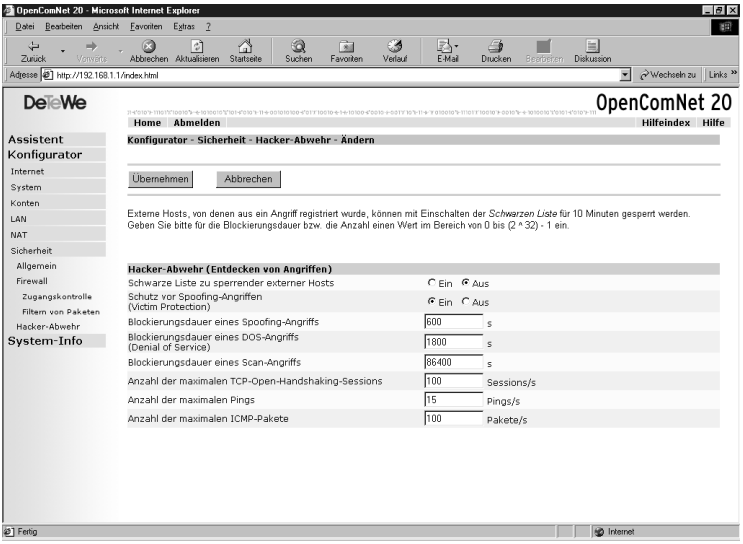
Haben Sie alle Angaben gemacht, klicken Sie auf **Übernehmen**.

* Die Protokollnummer kennzeichnet das in der darüberliegenden Transportebene verwendete Protokoll (TCP = 6, UDP = 17).

Hacker-Abwehr



Sie sehen jetzt die aktuellen Einstellungen. Wollen Sie Änderungen in den Einstellungen vornehmen klicken Sie auf **Ändern**.


OpenComNet 20 - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Bearbeiten Diskussion
Adresse http://192.168.1.1/index.html
Wechseln zu Links
DeTeWe
OpenComNet 20
Home Abmelden
Hilfeindex Hilfe
Assistent
Konfigurator
Internet
System
Konten
LAN
NAT
Sicherheit
Allgemein
Firewall
Zugangskontrolle
Filtern von Paketen
Hacker-Abwehr
System-Info
Konfigurator - Sicherheit - Hacker-Abwehr - Ändern
Übernehmen
Abbrechen
Externe Hosts, von denen aus ein Angriff registriert wurde, können mit Einschalten der Schwarzen Liste für 10 Minuten gesperrt werden. Geben Sie bitte für die Blockierungsdauer bzw. die Anzahl einen Wert im Bereich von 0 bis (2 ^ 32) - 1 ein.
Hacker-Abwehr (Entdecken von Angriffen)
Schwarze Liste zu sperrender externer Hosts Ein Aus
Schutz vor Spoofing-Angriffen (Victim Protection) Ein Aus
Blockierungsdauer eines Spoofing-Angriffs 600 s
Blockierungsdauer eines DOS-Angriffs (Denial of Service) 1800 s
Blockierungsdauer eines Scan-Angriffs 86400 s
Anzahl der maximalen TCP-Open-Handshaking-Sessions 100 Sessions/s
Anzahl der maximalen Pings 15 Pings/s
Anzahl der maximalen ICMP-Pakete 100 Pakete/s
Fertig
Internet

- Schwarze Liste zu sperrender externer Hosts
  Wenn die Firewall einen Angriff von einem Host registriert hat, so wird der Zugriff von diesem Host auf den Router für 10 Minuten gesperrt.

- Schutz vor Spoofing-Angriffen (Victim Protection)
  Spoofing-Angreifer beobachten mit welchen Servern ein Rechner kommuniziert und tarnen Ihre Attacke anschließend als normale Kommunikation. Aus diesem Grunde sollte dieser Schutz immer aktiviert sein.

- Blockierungsdauer eines Spoofing-Angriffs
  Zeitdauer in Sekunden, in der die Firewall Pakete an das Spoofing-Opfer im LAN blockiert.

- Blockierungsdauer eines DoS-Angriffs (Denial of Service)
  Bei einem DoS-Angiff werden alle verdächtigen Hosts für diese Zeitdauer in Sekunden blockiert.

- Blockierungsdauer eines Scan-Angriffs
  Die Firewall erkennt das Scannen von verdächtigen Hosts, um offene Ports zu finden und blockiert diese Hosts für die angegebene Zeitdauer in Sekunden.

- Anzahl der maximalen TCP-Open-Handshaking-Sessions
  Hier wird die maximale Anzahl von offenen (also nicht beendeten) TCP-Verbindungen pro Sekunde eingestellt, die von der Firewall erlaubt sind, bevor ein „SYN Flood“ erkannt wird. „SYN Flood“ ist ein DoS (Denial of Service) Angriff.

- Anzahl der maximalen Pings
  Hier wird die maximale Anzahl von Pings pro Sekunde eingestellt, die von der Firewall erlaubt sind, bevor ein „Echo Storm“ erkannt wird. „Echo Storm“ ist ein DoS (Denial of Service) Angriff.

- Anzahl der maximalen ICMP-Pakete
  Hier wird die maximale Anzahl von ICMP-Paketen pro Sekunde eingestellt, die von der Firewall erlaubt sind, bevor ein „ICMP Flood“ erkannt wird. „ICMP Flood“ ist ein DoS (Denial of Service) Angriff.

Machen Sie in den entsprechenden Feldern die Eintragungen. Klicken Sie danach auf **Übernehmen**.

Besondere Leistungsmerkmale

UPnP (Universal Plug and Play)
Ihr OpenComNet 20 unterstützt UPnP. Wenn Sie auf Ihren PCs im LAN Betriebssysteme einsetzen, die ebenfalls UPnP unterstützen (z. B. Windows XP), werden alle Geräte oder Anwendungen die Ihrem Netzwerk neu hinzugefügt werden und ihrerseits ebenfalls UPnP-kompatibel sind, automatisch erkannt und Ihren Fähigkeiten entsprechend konfiguriert. Auch die entsprechende Netzwerkkonfiguration erfolgt dann automatisch. Wenn die Anwendung z. B. virtuelle Server-Funktionen benötigt, wird von UPnP automatisch ein entsprechendes Port Forwarding eingerichtet.
Gehen Sie wie folgt vor, wenn Sie UPnP auf Ihren Windows XP-Rechnern aktivieren oder deaktivieren wollen:

- Wählen Sie -> Start -> **Systemsteuerung**
- Doppelklick auf **Software**
- Klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**
- Scrollen Sie auf **Netzwerkdienste**, selektieren Sie diese und klicken Sie auf **Details ...** .
- Sie können jetzt **Universelles Plug & Play** aktivieren oder abschalten.
- Bestätigen Sie Ihre Auswahl mit **OK**.

Um UPnP nutzen zu können, müssen Sie darüberhinaus die XP-Firewall-Dienste auf Ihren Rechnern deaktivieren.
Gehen Sie hierzu wie folgt vor:

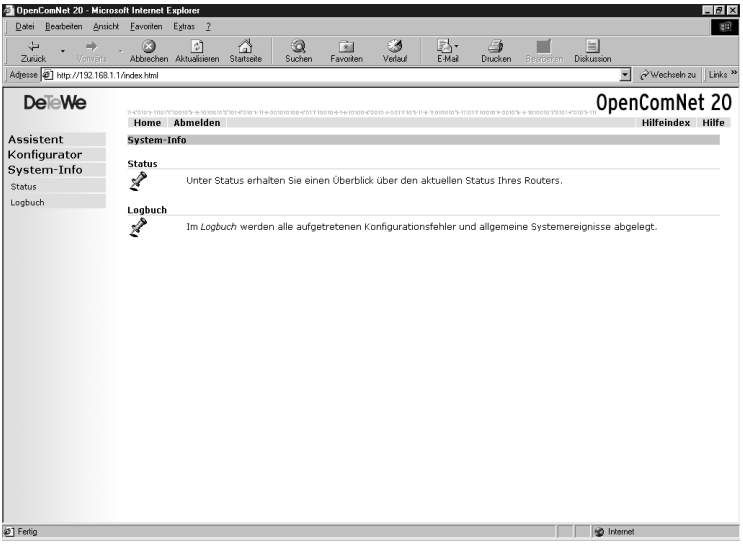
- Wählen Sie -> Start -> **Systemsteuerung**
- Doppelklick auf **Netzwerkverbindungen**
- Doppelklick auf **LAN-Verbindung**
- Wählen Sie **Eigenschaften**
- Wählen Sie die Karteikarte **Erweitert** und deaktivieren Sie die Checkbox „Diesen Computer und das Netzwerk schützen, indem das Zugreifen auf diesen Computer vom Internet eingeschränkt oder verhindert wird".
- Bestätigen Sie Ihre Auswahl mit **OK**.

Hinweis

UPnP kann das Einrichten einer Applikation oder eines Gerätes im LAN automatisieren und damit sehr benutzerfreundlich gestalten. Es stellt jedoch auch eine Sicherheitslücke für potentielle Angreifer dar. Sie müssen selber entscheiden, was Ihnen wichtiger ist und diese Funktion ggf. auf Ihren Rechnern deaktivieren. Eine zentrale Deaktivierung über den OpenComNet 20 ist derzeit nicht möglich.
Sie können aber auch eine Firmware **ohne** UPnP Unterstützung einsetzen. Die Firmware befindet sich auf der Produkt CD. Die Installation erfolgt wie im Kapitel - **Firmware Update** - beschrieben. Wählen Sie als Daten-Quelle statt des Links unter **Firmware-Datei Auswählen/Durchsuchen** die Produkt CD.

System-Info

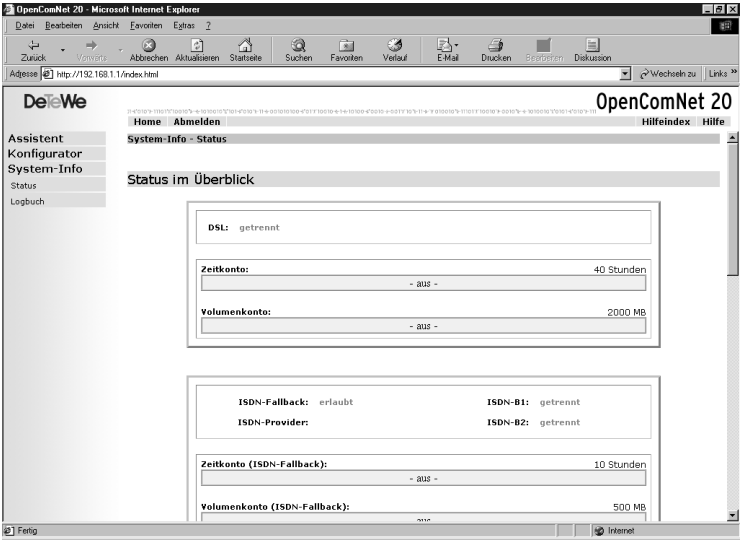
Wählen Sie aus dem Hauptmenü in der linken Spalte **System-Info**.



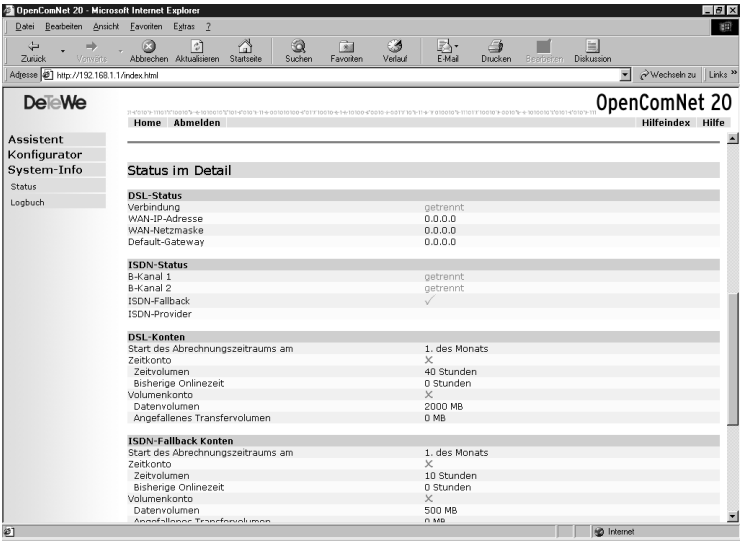
System-Info

Status	Zeigt den aktuellen Status des Routers an.
Logbuch	Die Logbücher zeichnen Aktionen während des Betriebes vom OpenComNet 20 auf. Diese Informationen sind sehr hilfreich bei einer Fehlersuche, wenn Sie allerdings alle Möglichkeiten ausschöpfen, erzeugen Sie einen sehr großen Datenbestand.

Status

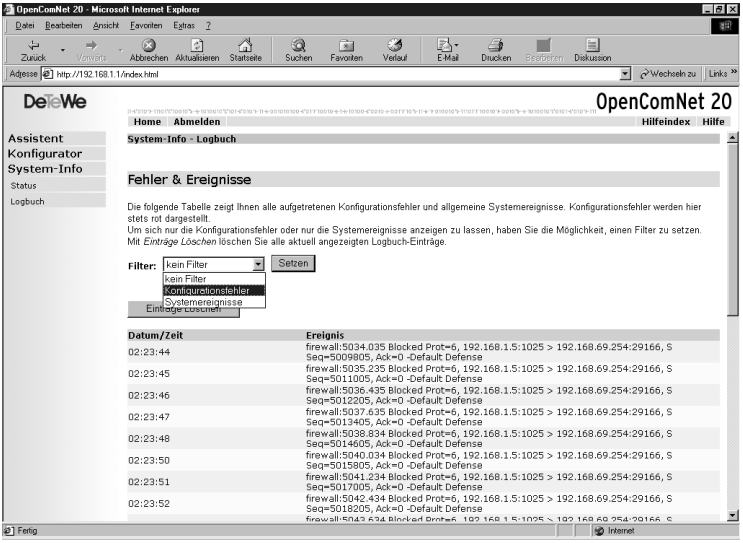


Sie sehen jetzt die aktuellen Einstellungen. Benutzen Sie auch die Rollbalken um das ganze Fenster anzuzeigen.



Schließen Sie dieses Fenster indem Sie im Browserfenster auf **Zurück** klicken.

Logbuch.


OpenComNet 20 - Microsoft Internet Explorer
DeTeWe
OpenComNet 20
Home
Abmelden
Hilfeindex
Hilfe
Assistent
Konfigurator
System-Info
Status
Logbuch
System-Info - Logbuch
Fehler & Ereignisse
Die folgende Tabelle zeigt Ihnen alle aufgetretenen Konfigurationsfehler und allgemeine Systemereignisse. Konfigurationsfehler werden hier stets rot dargestellt.
Um sich nur die Konfigurationsfehler oder nur die Systemereignisse anzeigen zu lassen, haben Sie die Möglichkeit, einen Filter zu setzen.
Mit Einträge Löschen löschen Sie alle aktuell angezeigten Logbuch-Einträge.
Filter:
kein Filter
Setzen
kein Filter
Konfigurationsfehler
Systemereignisse
Einträge Löschen
Datum/Zeit
Ereignis
02:23:44 firewall:5034.035 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5009805, Ack=0 -Default Defense
02:23:45 firewall:5035.235 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5011005, Ack=0 -Default Defense
02:23:46 firewall:5036.435 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5012205, Ack=0 -Default Defense
02:23:47 firewall:5037.635 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5013405, Ack=0 -Default Defense
02:23:48 firewall:5038.834 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5014605, Ack=0 -Default Defense
02:23:50 firewall:5040.034 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5015805, Ack=0 -Default Defense
02:23:51 firewall:5041.234 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5017005, Ack=0 -Default Defense
02:23:52 firewall:5042.434 Blocked Prot=6, 192.168.1.5:1025 > 192.168.69.254:29166, S Seq=5018205, Ack=0 -Default Defense
Fertig
Internet

Sie sehen jetzt die Aufzeichnung alle Aktionen. Benutzen Sie auch die Rollbalken um das ganze Fenster anzuzeigen. Sie können bei Bedarf über das Menü Filter setzen, um nur Konfigurationsfehler oder Systemereignisse anzuzeigen.

Die Schaltfläche **Einträge löschen** löscht alle aktuellen Einträge.

Installation des Druckertreibers für den Netzwerkdrucker

Windows 2000

- Schließen Sie Ihren Netzwerkdrucker an den Printerport des OpenComNet 20 an und schalten Sie ihn ein.
- Wählen Sie Start -> Einstellungen -> **Drucker**.
- Doppelklick auf **Neuer Drucker**.
- Klicken Sie auf **Weiter**.
- Wählen Sie **Lokaler Drucker**, deaktivieren Sie die automatische Druckererkennung und klicken Sie auf **Weiter**.
- Markieren Sie **Einen neuen Anschluss erstellen** und wählen Sie den Typ **Standard TCP/IP-Port**.
- Klicken Sie auf **Weiter**.
- Geben Sie die IP-Adresse des OpenComNet 20 ein (Werkseinstellung 192.168.1.1) und klicken Sie auf **Weiter**.
- Selektieren Sie **Benutzerdefiniert** und klicken Sie auf **Einstellungen**.
- Wählen Sie das Raw-Protokoll, aktivieren Sie **SNMP** und klicken Sie auf **OK**.
- Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.
- Wählen Sie im linken Menü den Druckerhersteller, im rechten den Druckertyp (wenn Ihr Druckertyp nicht angeboten wird, können Sie den Treiber auch von einem Datenträger laden) und klicken Sie auf **Weiter**.
- Klicken Sie erneut auf **Weiter**.
- Wählen Sie **Freigeben als:**, geben Sie einen Namen Ihrer Wahl ein und klicken Sie auf **Weiter**.
- Geben Sie jetzt den Druckerstandort (z. B. Keller), einen Kommentar zur Druckerausstattung (z. B. Farbdrucker) ein und klicken Sie auf **Weiter**.
- Wählen Sie **Ja** für „Soll eine Testseite gedruckt werden?“, klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**. Es wird eine Testseite gedruckt.

Windows XP

- Schließen Sie Ihren Netzwerkdrucker an den Printerport des OpenComNet 20 an und schalten Sie ihn ein.
- Wählen Sie Start -> **Drucker und Faxgeräte**.
- Klicken Sie auf **Drucker hinzufügen** und auf **Weiter**.
- Wählen Sie **Lokaler Drucker**, deaktivieren Sie **Plug&Play…** und klicken Sie auf **Weiter**.
- Wählen Sie **Einen neuen Anschluss erstellen**, selektieren Sie aus dem Menü **Standard TCP/IP-Port** und klicken Sie auf **Weiter**.
- Klicken Sie erneut auf **Weiter**.
- Geben Sie die IP-Adresse des OpenComNet 20 ein (Werkseinstellung 192.168.1.1) und klicken Sie auf **Weiter**.
- Wählen Sie **Benutzerdefiniert** und klicken Sie auf **Einstellungen**.

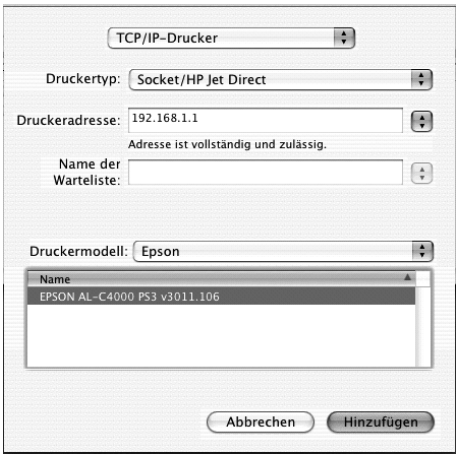
- Wählen Sie das Raw-Protokoll, aktivieren Sie **SNMP** und klicken Sie auf **OK**.
- Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.
- Wählen Sie im linken Menü den Druckerhersteller, im rechten den Druckertyp (wenn Ihr Druckertyp nicht angeboten wird, können Sie den Treiber auch von einem Datenträger laden) und klicken Sie auf **Weiter**.
- Klicken Sie erneut auf **Weiter**.
- Wählen Sie **Freigabename**, geben Sie einen Namen Ihrer Wahl ein und klicken Sie auf **Weiter**.
- Geben Sie jetzt den Druckerstandort (z. B. Keller), einen Kommentar zur Druckerausstattung (z. B. Farbdrucker) ein und klicken Sie auf **Weiter**.
- Wählen Sie **Ja** für „eine Testseite drucken“, klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**. Es wird eine Testseite gedruckt.

Windows 98 SE

- Zum Zeitpunkt der Entwicklung von Windows 98 war die Unterstützung von Print-Servern noch nicht vorgesehen. Im Nachhinein wurden für einzelne Drucker herstellerseitig Spezialtreiber entwickelt. Im Internet finden sich darüberhinaus Sharewareprogramme zur Nutzung von Druckern unter Windows 98 über Printserver. Bitte haben Sie Verständnis dafür, dass wir auf diesbezügliche Einzelheiten in dieser Bedienungsanleitung nicht eingehen können, da es sich um Fremdlösungen handelt.

Mac OS X

- Schließen Sie Ihren Netzwerkdrucker an den Printerport des OpenComNet 20 an und schalten Sie ihn ein.
- Öffnen Sie die Systemeinstellung **Drucken & Faxen**.
- Klicken Sie in **Drucken** und anschließend in **Drucker konfigurieren**.
  Wenn der Drucker bereits in der Druckerliste angezeigt wird, markieren Sie das Feld „Im Menü“, um ihn in der Liste der verfügbaren Drucker hinzuzufügen. Das Einblendmenü „Drucker“ wird angezeigt, wenn Sie den nächsten Druckauftrag senden.
- Wählen Sie **Drucker** und dann **Drucker hinzufügen**.
- Wählen Sie aus dem Einblendmenü **TCP/IP-Drucker**.
- Wählen Sie aus dem Einblendmenü „Druckertyp“ aus der Liste ein geeignetes Druckprotokoll aus.
- Geben Sie die IP-Adresse oder den DNS-Namen des Routers in das Feld „Druckeradresse“ ein (oder wählen Sie die Adresse aus der Liste aus).



- Geben Sie den Namen der Druckerwarteliste (falls erforderlich) in das Feld „Warteliste ein. Wenn Sie den Namen der Warteliste nicht kennen, wenden Sie sich an Ihren Netzwerkadministrator.
- Wenn Sie spezielle Druckerfunktionen verwenden wollen, wählen Sie das betreffende Objekt für Ihren Drucker aus dem Einblendmenü „Druckermodell“ aus. Wählen Sie anschließend Ihren Drucker aus der Liste „Name“ aus.
- Klicken Sie in **Hinzufügen**.
- Der Drucker wird in der Druckerliste als Standarddrucker (in Fettdruck) angezeigt. Er wird zudem im Einblendmenü „Drucker“ angezeigt, wenn Sie ein Dokument zum Drucken senden wollen.

Software installieren

Informationen über die Software

Auf der beiliegenden CD-ROM finden Sie die folgende Software:

- **Betriebssoftware** für den OpenComNet 20 beinhaltet die notwendige Software zum Betrieb des OpenComNet 20 incl. CAPI, CAPI Port und CAPI Control.
- **WinSuite** ist ein Programmpaket, das Ihnen die folgenden Anwendungen auf Ihrem PC zur Verfügung stellt:
  - WinSuite **PC-Telefonie** ermöglicht Ihnen die Einrichtung und Nutzung eines komfortablen PC-Telefons.
  - WinSuite **Anrufliste** zeigt Ihnen den Status von entgangenen und selbst gewählten Anrufen an.
  - WinSuite **MMS-Center** ermöglicht das Senden/Empfangen und Speichern von Festnetz-MMS, sofern vom Netzanbieter unterstützt.
  - WinSuite **FaxCenter** ermöglicht Ihnen das Senden und Empfangen von Faxnachrichten sowie die Verwaltung eingegangener Faxnachrichten.
  - WinSuite **EurofileTransfer** dient dazu, Dateien im EuroFile-Transfer-Standard von einem anderen PC zu empfangen oder selbst an einen anderen PC zu senden.
  - WinSuite **SMSCenter** : Sie können Textnachrichten versenden. Die eigene Rufnummer (Absender) ist konfigurierbar.
  - Der WinSuite **PC-Anrufbeantworter** zeichnet kommende Anrufe auf, die Sie direkt aus der Anrufbeantwortersoftware oder aus der Anrufliste (Journal) abhören können.
  - WinSuite **Adressbuch**
  - WinSuite **Journal**

Starten des Installationsprogramms

Das Installationsprogramm startet nach Einlegen der CD automatisch.
Sollte aufgrund der Konfiguration Ihres PCs das Installationprogramm nicht selbsttätig starten, rufen Sie das Programm durch Doppelklick auf das Symbol „Setup.exe“ im Hauptverzeichnis der CD auf.

Konfiguration Telefonanwendung

PC Voraussetzungen

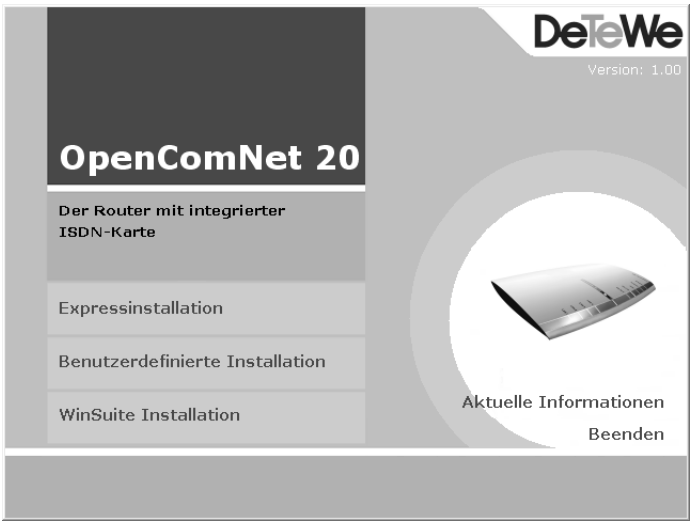
- IBM-kompatibler PC mit Festplatte und CD-ROM-Laufwerk
- Taktfrequenz von 266 MHz oder höher
- Arbeitsspeicher mindestens 256 MB
- Microsoft Windows 98 SE/Me/2000/XP
- freie Festplattenkapazität von min. 20 MByte
- Für AB-Nutzung: Vollduplex Soundkarte (mit Mikrofon)

Hinweis

Vor der Installation der Software müssen Sie bestehende CAPI-/TAPI-Treiber anderer Produkte unbedingt entfernen.
Installieren Sie die WinSuite vor der Expressinstallation oder der Benutzerdefinierten Installation, so wird die Installation der CAPI- und TAPI-Treiber automatisch gestartet, da diese für den Betrieb der Kommunikationssoftware unverzichtbar sind.

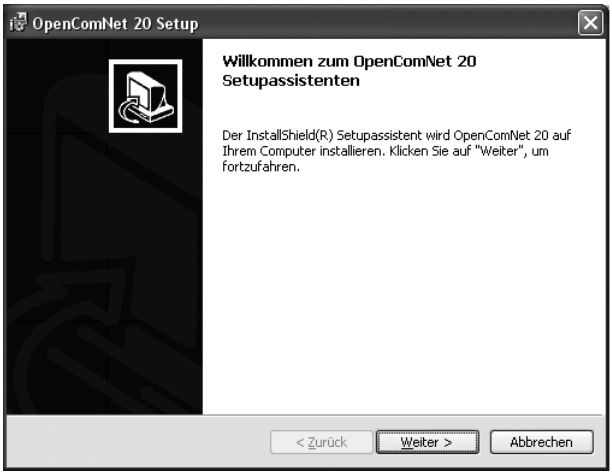
Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein. Klicken Sie auf den Eintrag **OpenComNet 20**.

Installation der Software

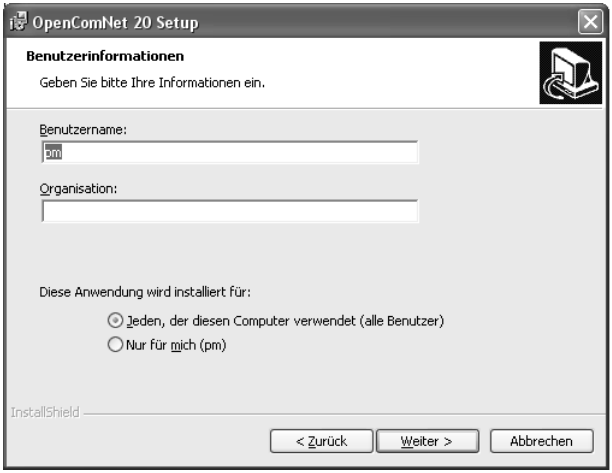


Wählen Sie **Expressinstallation**.

Der Installationsassistent


OpenComNet 20 Setup
Willkommen zum OpenComNet 20 Setupassistenten
Der InstallShield(R) Setupassistent wird OpenComNet 20 auf Ihrem Computer installieren. Klicken Sie auf "Weiter", um fortzufahren.
< Zurück
Weiter >
Abbrechen

Folgen Sie den Anweisungen des Setupassistenten.



Machen Sie die Angaben in den Feldern **Benutzername** und **Organisation**. Aktivieren Sie anschließend eine der beiden Checkboxen. Klicken Sie dann auf **Weiter** und folgen Sie den Anweisungen bis **Fertigstellen**. Führen Sie anschließend einen Neustart durch.

Nach erfolgreicher Installation finden Sie in der Windows Taskleiste das CAPIControl Icon .

CAPIControl Einstellungen

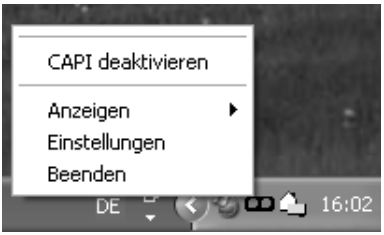
Das Hilfsprogramm CAPI Control bietet Ihnen neben umfangreichen Informationen über eine bestehende Verbindung auch eine Vielzahl von Kontroll- und Einstellmöglichkeiten für die CAPI-Schnittstelle.
In der rechten unteren Ecke der Windows-Taskleiste befindet sich das abgebildete Icon in Form von je einer LED für jeden B-Kanal.

Durch die Färbung des Icons wird der Zustand der CAPI-Schnittstelle angezeigt.

Die Farben haben die folgenden Bedeutungen:

rot	-	deaktiviert
gelb	-	keine Verbindung zum Gerät
grau	-	bestehende Verbindung zum Gerät
grün	-	bestehende Verbindung zum ISDN

Nach Anklicken mit der rechten Maustaste können Sie aus dem aufklappenden Menü die folgenden Programme aufrufen bzw. Einstellungen vornahmen:

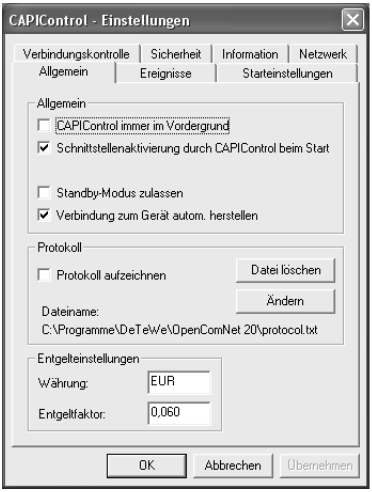


CAPI deaktivieren/aktivieren: je nach aktuellem Zustand können Sie entweder die CAPI aus- oder einschalten.

Anzeigen: sie können zwischen „kompakt", „standard" und „erweitert" wählen, wie umfangreich die Anzeigen für die aktive CAPI-Verbindung sein sollen.

Einstellungen öffnet das Hilfsprogramm CAPIControl, mit dem Sie verschiedene Einstellungen für die CAPI-Schnittstelle vornehmen können.

Sie sehen die Registerkarte **CAPIControl Einstellungen**. Einige Einstellungen sind bereits durch den Installationsassistenten erfolgt.



Aktualisieren Sie die Vorgaben in den Feldern Währung und Entgeltfaktor. Klicken Sie danach auf **Übernehmen**.

Wählen Sie die nächste Registerkarte **Netzwerk** aus.

Sie sehen im Feld **IP-Adresse** die aktuelle LAN-IP-Adresse des OpenComNet 20. Sofern Sie diese Adresse bei der Konfiguration Ihres OpenComNet 20 geändert haben, müssen Sie sie hier ebenfalls ändern. Klicken Sie anschließend auf **OK**.

Wählen Sie die nächste Registerkarte **Sicherheit** aus.

Nach Klicken auf **Neu** können Sie einen Namen für die Verbindung und eine Rufnummer eingeben, über die eine Wählverbindung aufgebaut werden darf.
Es können mehrere Nummern eingegeben werden. Aktivieren Sie die **Verbindungsüberwachung** durch Klicken in die entsprechende Checkbox ✔. Dort erscheint ein Häkchen, wenn die Funktion aktiviert ist.

Haben Sie Änderungen vorgenommen klicken Sie danach auf **Übernehmen**.

Wählen Sie die nächste Registerkarte **Verbindungsprotokolle** aus.

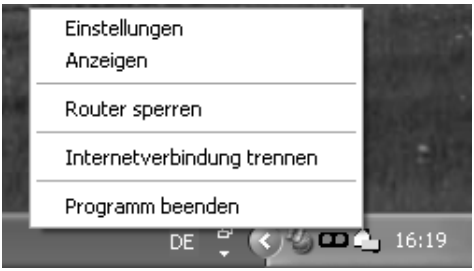
Sie können für einzelne Verbindungen ein Protokoll führen lassen, in dem die Onlinezeit für die Rufnummer festgehalten wird. Alle Rufnummer sind in einer Liste aufgeführt. Wollen Sie zu einer Rufnummer Änderungen durchführen, aktivieren Sie den Eintrag in der Liste und klicken Sie auf **Bearbeiten**. Wollen Sie der Liste eine neue Rufnummer hinzufügen, klicken Sie auf **Neu**.

Wenn Sie jetzt auf **Ändern** klicken, können Sie eine neue Klangdatei für den Alarm auswählen.

Über die Schaltfläche **Abspielen** können Sie sich den Klang anhören. Bestätigen Sie Ihre Auswahl mit **OK**.

HomeNet Control Einstellungen

Beim Aufruf eines Browsers (z. B. Internet Explorer oder Netscape Communicator) oder eines E-Mail-Programms auf dem an den OpenComNet 20 angeschlossenen PC wird automatisch eine Verbindung zum Internet hergestellt.
Eine bestehende Internetverbindung erkennen Sie an dem grünen Symbol „HomeNet Control“ ( ) in der Windows-Taskleiste.



Zum manuellen Trennen der Internet-Verbindung klicken Sie mit der **rechten** Maustaste auf das abgebildete Symbol „HomeNet Control“ ( ) unten rechts in der Windows-Taskleiste und wählen **Internetverbindung trennen** aus.

Unter **Einstellungen** legen Sie die Anzeigeoptionen für HomeNetControl fest.

Anzeigen gibt Informationen über die aktuelle Verbindung wie Datenübertragungsgeschwindigkeit, Dauer der Verbindung und gesendete bzw. empfangene Datenmengen.

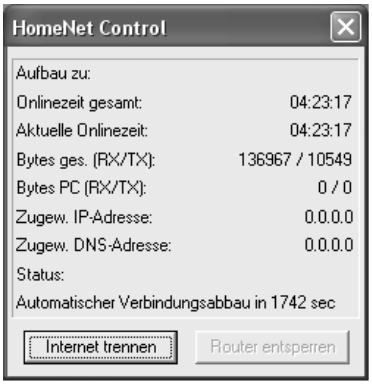
Mit **Router sperren** können Sie die automatische Internet-Einwahl über HomeNetControl sperren bzw. freigeben. So können Sie verhindern, dass sich Applikationen außerhalb der von Ihnen gewünschten Nutzungszeiten selbsttätig mit dem Internet verbinden und Verbindungskosten verursachen.

Mit **Programm beenden** verschwindet das Icon bis zum nächsten Systemstart aus der Taskleiste.

Klicken Sie auf **Einstellungen**.

Sie können einstellen, ob das Fenster HomeNet Control immer im Vordergrund angezeigt wird. Darüberhinaus können Sie die registrierte **Onlinezeit löschen**. Unter **NDIS-Blockierung** können Sie eine Parallelverbindung zum Internet über den Router verhindern, wenn bereits eine DFÜ-Verbindung existiert. Die Aktivierung wird empfohlen.

Schließen Sie das Fenster und klicken Sie danach auf **Anzeigen**.



Das Fenster zeigt Informationen über die aktuelle Verbindung wie Datenübertragungsgeschwindigkeit, Dauer der Verbindung, gesendete bzw. empfangene Datenmengen und die WAN-seitige IP- und DNS-Adresse Ihre OpenComNet 20.

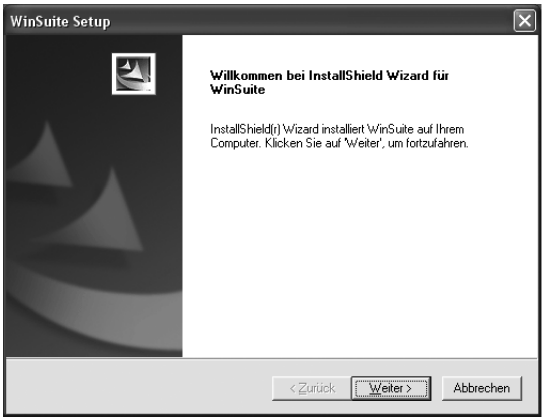
Schließen Sie das Fenster.

Kommunikationssoftware installieren

Konfigurationsassistent WinSuite

Legen Sie, sofern noch nicht geschehen, die Produkt-CD in das CD-ROM-Laufwerk ein. Klicken Sie im Explorer auf den Eintrag **Setup.exe**.

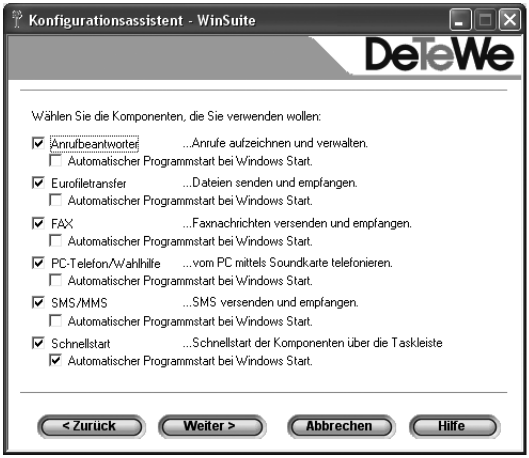
Wählen Sie **WinSuite Installation** aus.
Bei der Erstinstallation wird der Konfigurationsassistent automatisch gestartet, danach können Sie ihn jederzeit über „Start -> Programme ->WinSuite“ erreichen.


WinSuite Setup
Willkommen bei InstallShield Wizard für WinSuite
InstallShield(r) Wizard installiert WinSuite auf Ihrem Computer. Klicken Sie auf 'Weiter', um fortzufahren.
< Zurück
Weiter >
Abbrechen

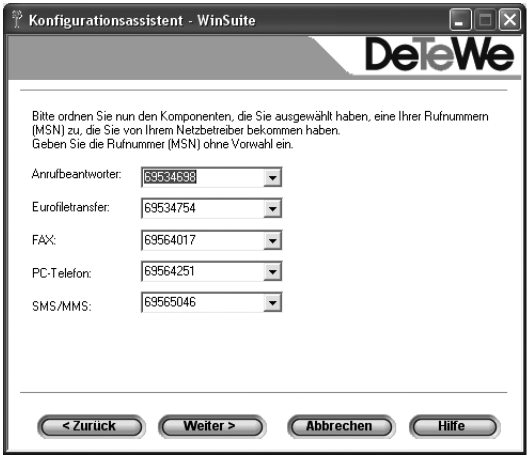
Klicken Sie auf **Weiter**, folgen Sie den Anweisungen des Assistenten und beenden Sie die Installation mit **Fertigstellen**.

Konfigurationsassistent - WinSuite
DeTeWe
Mit Hilfe dieses Konfigurationsassistenten können Sie die verschiedenen Komponenten vom WinSuite konfigurieren. Hierzu sind einige Angaben zu dem ISDN-Anschluss, an dem Sie Ihr ISDN-Gerät betreiben, notwendig.
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter**.


Konfigurationsassistent - WinSuite
DeTeWe
Wählen Sie die Komponenten, die Sie verwenden wollen:
Anrufbeantworter ...Anrufe aufzeichnen und verwalten.
Automatischer Programmstart bei Windows Start.
Eurofiletransfer ...Dateien senden und empfangen.
Automatischer Programmstart bei Windows Start.
FAX ...Faxnachrichten versenden und empfangen.
Automatischer Programmstart bei Windows Start.
PC-Telefon/Wahlhilfe ...vom PC mittels Soundkarte telefonieren.
Automatischer Programmstart bei Windows Start.
SMS/MMS ...SMS versenden und empfangen.
Automatischer Programmstart bei Windows Start.
Schnellstart ...Schnellstart der Komponenten über die Taskleiste
Automatischer Programmstart bei Windows Start.
< Zurück
Weiter >
Abbrechen
Hilfe

Wählen Sie die Komponenten aus, die Sie benötigen. Durch Markierung der Checkbox (✓) **Automatischer Programmstart...** können Sie die Anwendungen definieren, die automatisch beim Starten von Windows aktiviert werden sollen. Dadurch brauchen Sie die favorisierten Anwendungen nicht mehr manuell zu starten.
Klicken Sie anschließend auf **Weiter**.


Konfigurationsassistent - WinSuite
DeTeWe
Bitte ordnen Sie nun den Komponenten, die Sie ausgewählt haben, eine Ihrer Rufnummern (MSN) zu, die Sie von Ihrem Netzbetreiber bekommen haben.
Geben Sie die Rufnummer (MSN) ohne Vorwahl ein.
Anrufbeantworter: 69534698
Eurofiletransfer: 69534754
FAX: 69564017
PC-Telefon: 69564251
SMS/MMS: 69565046
< Zurück
Weiter >
Abbrechen
Hilfe

Für einen ISDN Anschluss stehen Ihnen mehrere Rufnummern (MSN) zur Verfügung.

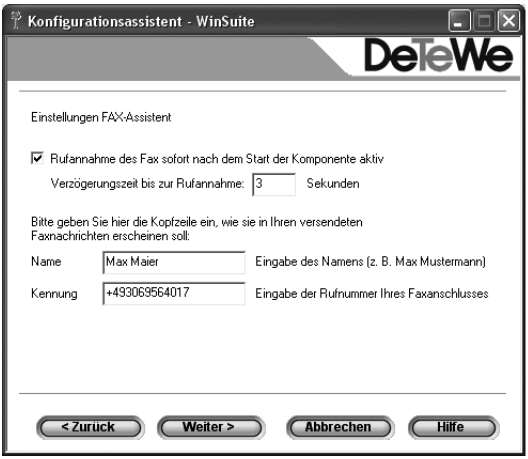
Ordnen Sie die Rufnummern den entsprechenden Programmteilen zu. Besonderheit: Geben Sie beim PC-Telefon keine Rufnummer (MSN) ein, werden alle ankommenden Anrufe signalisiert.
Klicken Sie auf **Weiter**.

Soll der Anrufbeantworter sofort nach dem Programmstart in Betrieb sein, aktivieren Sie die Checkbox (✓).
Tragen Sie die Zeit ein, die bis zur Rufannahme vergehen darf und die Zeit, die für eine Aufnahme zur Verfügung stehen soll.
Soll bei einem Anruf auch ein akustisches Signal erzeugt werden, aktivieren Sie die Checkbox (✓).

Klicken Sie auf **Weiter**.

Konfigurationsassistent - WinSuite
DeTeWe
Einstellungen Eurofiletransfer
Rufannahme des EFT sofort nach dem Start der Komponente aktiv
Servername:
Eurosoft
Den Servernamen (max. 12 Zeichen) des Eurofiletransfer-Servers müssen Sie eingeben, um mit der Applikation im Servermode arbeiten zu können.
< Zurück
Weiter >
Abbrechen
Hilfe

Soll Ihr Rechner sofort nach dem Programmstart als EFT-Server für andere Benutzer zur Verfügung stehen, aktivieren Sie die Checkbox (✓).
Vergeben Sie hier einen Namen für Ihren Rechner wenn er als Eurofile-Server arbeiten soll.
Klicken Sie auf **Weiter**.



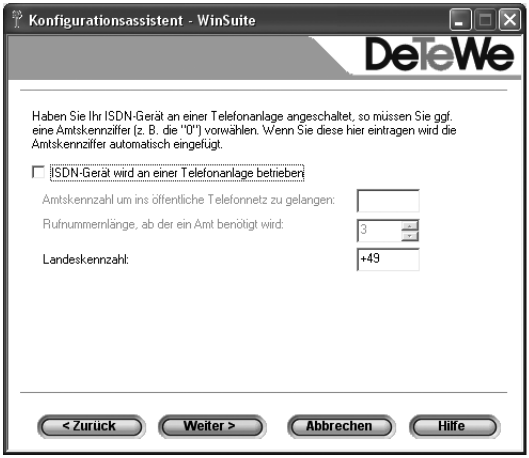
Soll Ihr Rechner sofort nach dem Programmstart für den Faxempfang bereit sein, aktivieren Sie die Checkbox (✓).
Tragen Sie die Zeit ein, die bis zur Rufannahme vergehen darf.
Machen Sie die Angaben für die Kopfzeile, die auf von Ihnen versendeten Faxen erscheinen soll.
Klicken Sie auf **Weiter**.

Konfigurationsassistent - WinSuite
DeTeWe
Einstellungen für das das PC-Telefon (CAPI) und für die Wahlhilfe (TAPI)
Einstellungen CAPI
Soundkarte
SoundMAX Digital Audio
Bei korrekter Installation der Software können Sie Ihre Soundkarte aus der angebotenen Liste auswählen.
< Zurück
Weiter >
Abbrechen
Hilfe

Wählen Sie unter dem Rollbalken den Soundkartentyp aus (die Installationssoftware sollte die eingebaute Soundkarte bereits erkannt haben).
Klicken Sie auf **Weiter**.

Hinweis

Wenn Sie über Ihren Rechner auch telefonieren möchten benötigen Sie eine Soundkarte und ein Headset. Wollen Sie das Headset nicht ständig tragen und trotzdem die Anrufsignalisierung nicht verpassen, benötigen Sie noch einen Lautsprecher.


Konfigurationsassistent - WinSuite
DeTeWe
Haben Sie Ihr ISDN-Gerät an einer Telefonanlage angeschaltet, so müssen Sie ggf. eine Amtskennziffer (z. B. die "0") vorwählen. Wenn Sie diese hier eintragen wird die Amtskennziffer automatisch eingefügt.
ISDN-Gerät wird an einer Telefonanlage betrieben
Amtskennzahl um ins öffentliche Telefonnetz zu gelangen:
Rufnummernlänge, ab der ein Amt benötigt wird:
3
Landeskennzahl:
+49
< Zurück
Weiter >
Abbrechen
Hilfe

Ist Ihr ISDN Adapter nicht direkt an einen NTBA sondern an eine Telefonanlage angeschlossen, aktivieren Sie die Checkbox (✓).
Tragen Sie die Kennzahl für die Amtsholung ein (Hilfe finden Sie in der Bedienungsanleitung der Telefonanlage). Dadurch stellt die Software abgehenden externen Rufnummern die Amtskennziffer voran.
Klicken Sie auf **Weiter**.

Sie können die Eintragungen in bestehenden Adressbüchern mit der WinSuite nutzen. Aktivieren Sie die Checkbox(en) des entsprechenden Programms.
Klicken Sie auf **Weiter**.

Damit haben Sie die Grundeinstellungen vorgenommen.

Konfigurationsassistent - WinSuite
DeTeWe
Sie haben jetzt alle für die Konfiguration erforderlichen Daten eingegeben. Drücken Sie auf 'Fertig stellen', um die Konfiguration abzuschließen.
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Fertig stellen**.

Den Zugang zur WinSuite finden Sie jetzt über das Programmsymbol / -gruppe auf dem Desktop oder über „Start -> Programme -> WinSuite“.

Anhang

Technische Daten

Modell	ADSL Router
ADSL Modem	T1.413, G.DMT, G.lite, multi-mode
Abmessungen	255 mm (B) x 35 mm (H) x 170 mm (T)
Gewicht	470 g
Betriebstemperatur	+5° C bis +40° C, ortsfest, wettergeschützt
Lagertemperatur	-10° C bis 70° C
Netzwerkprotokoll	IP
Netzwerkanschlüsse	
- ADSL	RJ45-Anschluss für DSL Netzzugang (nach 1TR112V5.1, U-R2)
- ISDN	RJ45-Anschluss für ISDN extern (Euro ISDN Protokoll, DSS1)
- Fast Ethernet Switch	4 RJ45-Anschlüsse 10/100BaseT (auto MDI/MDIX)
- Printer Port	Sub-D25 Buchse für Centronics-Kabel (LPT)
Anzeigen (LED)	10
Netzspannung	230V~; 50Hz für Steckernetzgerät; nur Typ 4510742 verwenden
Leistungsaufnahme	typ. 10W (primär)

Pflege und Wartung

Ihr Gerät ist ein Produkt, das in Design und Ausführung höchsten Ansprüchen genügt. Es sollte daher mit Sorgfalt behandelt werden. Die folgenden Anregungen dienen dazu, Ihnen für lange Zeit die Freude an diesem Produkt zu erhalten.

Beachten Sie alle Sicherheitshinweise auf Seite 1.

Zum Reinigen des Gerätes ziehen Sie als erstes den Netzstecker. Wischen Sie das Gerät mit einem Antistatiktuch oder einem etwas angefeuchteten weichen Ledertuch ab, anschließend mit einem trockenen Tuch.

Hinweis: Sprühen Sie Ihr Gerät nie mit Reinigungs- oder Lösungsmittel ein.

Umwelteigenschaften und Entsorgung

Dieses Produkt wurde nach den gesetzlichen Forderungen und der Herstellerrichtlinie 2002 recycling- und umweltgerecht hergestellt.
Es wurde in Hinblick auf geringen Energieverbrauch, lange Brauchbarkeitsdauer und Servicefreundlichkeit unter Einsatz weniger, umweltschonender Werkstoffe und Bauteile entwickelt.
Helfen Sie mit, die Lebensdauer Ihrer Geräte zu verlängern, indem Sie die Sicherheitshinweise und die Pflege-/Wartungshinweise beachten.
Entsorgen Sie das Gerät entsprechend der behördlichen Auflagen. Führen Sie es der Wiederverwertung zu.
Elektronische Geräte gehören nicht in den Hausmüll.

Port Forwarding Regeln

Die anschließende Tabelle mit Port Forwarding-Regeln für die wichtigsten Kategorien stellt eine Momentaufnahme dar. Es handelt sich speziell bei den Spielen um Fremdanwendungen deren Daten sich jederzeit ändern können. Wir können daher für die aktuelle Richtigkeit nicht garantieren und empfehlen die Richtigkeit dieser Regeln vor Gebrauch im jeweiligen Herstellerhandbuch zu verifizieren.

- Kategorie Games

Name der Regel	Protokoll	Port Start	Port End
Alien vs. Predator	UDP	80	80
	UDP	2300	2400
	UDP	8000	8900
Asheron's call	UDP	9000	9001
	UDP	9004	9005
	UDP	9012	9013
Command & Conquer	TCP	4000	4000
	TCP/UDP	1140	1234
Dark Reign 2	TCP/UDP	26214	26214
Delta Force	TCP/UDP	3999	3999
DirectX (7,8) Games	TCP	47624	47624
	TCP	6073	6073
	TCP/UDP	2300	2400
Doom	TCP/UDP	666	666
Dune 2000	TCP	4000	4000
	TCP/UDP	1140	1234
Elite Force	UDP	26000	26000
	UDP	27500	27500
	UDP	27910	27910
	UDP	27960	27960
EverQuest	TCP	7000	7000
	UDP	1024	6000
Fighter Ace II	TCP/UDP	50000	50100

Name der Regel	Protokoll	Port Start	Port End
Half Life	TCP	27015	27015
Heretic II	TCP	28910	28910
Hexen II	UDP	26900	26905
Kali	UDP UDP	6666 2213	6666 2218
Motorhead	TCP/UDP TCP/UDP	16000 16010	16000 16030
MSN Gaming Zone	TCP TCP	6667 28800	6667 29000
Need for Speed 3	TCP	1030	1030
Need for Speed Porsche 2000	UDP	9442	9442
Outlaws	TCP	5310	5310
Quake 2 Server	UDP	27910	27910
Quake 3 Server	UDP	27660	27665
Rainbow Six	TCP	2346	2346
Rogue Spear	TCP	2346	2346
Starcraft	UDP	6112	6112
The Fallen Lords	UDP	3453	3453
Ultima	TCP TCP TCP TCP TCP	5001 7775 8800 9999 7875	5010 7777 8900 9999 7875
Unreal Tournament	UDP UDP UDP TCP	7777 27500 27900 8080	7781 27500 27900 8080

- Kategorie Audio/Video

Name der Regel	Protokoll	Port Start	Port End
Net2Phone	UDP	6613	6613
Netmeeting	TCP/UDP	1024	1064
	TCP	1503	1503
	TCP	1720	1720
	TCP	1731	1731
	TCP	522	522
	TCP	389	389
Quick Time 4 Server	TCP	6970	6970
	UDP	6970	7000

- Kategorie Applications

Name der Regel	Protokoll	Port Start	Port End
Carbon Copy	TCP	1680	1680
	UDP	1023	1679
Fernadministration Windows 2000	TCP	3638	3638
Gnutella	TCP	1214	1214
	TCP/UDP	6346	6346
Homebanking	TCP	3000	3000
Internet Relay Chat (IRC)	TCP	113	113
	TCP	6660	6669
	TCP	7000	7002
LapLink	TCP	1547	1547
Media Player	TCP	1755	1755
Netbios	TCP/UDP	137	139
PcAnywhere	TCP	5631	5631
	TCP	65301	65301
	UDP	22	22
	UDP	5632	5632
Radmin	TCP	4899	4899

Real Player	TCP	7070	7070
RemoteAnything	UDP TCP	3998 3999	3998 4000
T-Online Homebanking	TCP	866	866
VNC	TCP TCP TCP	5500 5800 5900	5500 5800 5900
Win2k Terminal	TCP/UDP	3389	3389

- Kategorie Servers

Name der Regel	Protokoll	Port Start	Port End
DNS Server	UDP	53	53
FTP Server	TCP	21	21
IMAP Server	TCP TCP TCP	143 585 993	143 585 993
IRC Server	TCP TCP TCP	6667 194 5100	6667 194 5100
LDAP Server	TCP TCP	389 636	389 636
Lotus Server	TCP	1352	1352
NNTP Server	TCP	119	119
POP2 Server	TCP	109	109
POP3 Server	TCP	110	110
Remotely Possible Server	TCP	799	799
SMTP Server	TCP	25	25
Telnet Server	TCP	23	23
Web Server (HTTP) (HTTPS)	TCP TCP	80 443	80 443

Glossar

ADSL
Abkürzung für Asymmetric Digital Subscriber Line
Übertragungstechnologie zur Realisierung breitbandiger Datenanschlüsse über das herkömmliche Kupferkabel-Anschlussnetz. Der so genannte Downstream-Kanal (in Richtung des Benutzers) ist breitbandig ausgelegt, der entgegengesetzte Upstream-Kanal (Rückkanal) ist hingegen relativ schmalbandig und in erster Linie für die Übertragung von Steuernachrichten vorgesehen.

CAPI
Abkürzung für Common ISDN Application Programming Interface. Eine Programmierschnittstelle, über die Windows-Programme auf die Funktionen von ISDN-Geräten am Computer zugreifen können.

CAPI Port Treiber
Ein Windows-Treiber, der eine serielle Schnittstelle mit angeschlossenem Modem simuliert. Damit können Programme, die ein konventionelles Modem erwarten, die ISDN-Schnittstelle nutzen.

Client
Rechner in einem Netzwerk, der Daten von einem Server beziehen kann.

DHCP (-Server/-Client)
Dynamic Host Configuration Protocol. Mittels DHCP können Rechner in einem LAN mit der erforderlichen Konfiguration zum Zugriff auf TCP/IP basierte Netzwerke von einer zentralen Stelle aus versorgt werden, die individuelle Konfiguration eines jeden Rechners entfällt.
So werden von dem Rechner, der die Informationen ausgibt (DCHP-Server) mindestens folgende, für den Internetzugang der Rechner (DHCP-Clients) notwendige Parameter vergeben: IP-Adresse, Netzwerkmaske, IP-Adresse des DNS-Servers oder DNS-Proxies und die IP-Adresse des Routers, der den Internetzugang herstellt (Default Gateway).
Per DHCP vergebene Adressen werden „geleast“, sie sind nur für eine bestimmte Zeit gültig. Rechtzeitig vor Ablauf dieser Zeitspanne (Lease Time) wird die Verlängerung der Gültigkeitsdauer oder die Übertragung eines neuen Datensatzes vereinbart. Dieser Ablauf geschieht zwischen DHCP-Client und -Server automatisch.

Dienstname (Service tag)
Der Dienstname kann dazu verwendet werden, zwischen mehreren Gegenstellen (PPPoE-Servern) auf der Provider-Seite zu unterscheiden. Üblicherweise wird dieser Eintrag nicht genutzt, da die Infrastruktur auf der Providerseite meist so ausgerichtet ist, dass die Verbindungen über den Benutzernamen (z. B. xxxxxxx@t-online.de oder xxxxxxx@de.aol.com) von einem PPPoE Server differenziert werden.
Wenn keine gegenteilige Information des ISPs vorliegt, sollte dieses Feld leer gelassen werden. Ein Eintrag, der von der Gegenseite nicht akzeptiert wird, führt dazu, dass keine PPPoE Verbindung hergestellt werden kann.

DNS
Abkürzung für Domain Name System.
Benennungsschema für Rechner im Internet. Ein Rechnername ist nach folgenden Prinzip aufgebaut: hostname.subdomain.domain.top-level - domain .Das gesamte Internet ist in eine Reihe von Bereichen aufgeteilt, die den Namen „Domain" bzw. „Toplevel Domain" tragen.

DNS-Adresse
IP-Adressen sind zwar für Rechner leicht zu handhaben, ein Mensch wird sich aber schwer tun, viele solcher Adressen zu behalten. Daher gibt es in einem Netzwerk üblicherweise einen Dienst, der für Menschen geeignete Namen in für Rechner geeignete IP-Adressen übersetzt. Dieser Dienst heißt Domain Name Service (DNS). Wenn Sie in Ihrem Browser also z. B. www.detewe.de eingeben, wird Ihr Rechner zunächst den DNS-Server bitten, die IP-Adresse zu diesem Namen nachzuschlagen. Anschließend wird er ein Paket an diese IP-Adresse schicken, um die betreffende Seite abzurufen. Möglicherweise kann der DNS-Server in Ihrem Netzwerk diese Anfrage aber nicht selbst beantworten, denn kein Rechner der Welt hat alle im Internet gültigen Namen und die zugehörigen IP-Adressen gespeichert. Es gibt aber ein ausgeklügeltes System, wie solche Anfragen durch das Internet bis zu einem Rechner weitergeleitet werden, der sie beantworten kann.

DoS-Attacke (Denial of Service)
Jedes Gerät (Server, Router, PC) im Netzwerk (LAN, Internet) kann nur eine begrenzte Menge von Daten verarbeiten (z. B. Menge gleichzeitiger http-Anfragen, äquvivalent zur Menge der Internet-Surfer, die diesen Server verwenden). Mit entsprechend manipulierten Datenpaketen kann z. B. der Server so beschäftigt werden, dass keine Daten mehr an die Nutzer abgegeben werden können. In einem solchen Fall „verweigert der Server die Arbeit" (denial of service) und beschäftigt sich nur noch mit den manipulierten Datenpaketen.

Filesharing
Applikationen für einen virtuellen Server - Filesharing Programme. Hierbei handelt es sich um Anwendungen, mit deren Hilfe man im Internet z. B. Musikstücke oder Spielfilme tauschen kann.

Firewall
(englisch, „Brandschutzmauer")
Eine Sicherheitseinrichtung zwischen zwei Computernetzwerken, die ein „sicheres Netz" vor unbefugten Zugriffen aus einem „unsicheren Netz" abschottet, ähnlich einer Brandschutzmauer, die die Ausbreitung eines Feuers stoppt oder zumindest erschwert. Firewalls werden beispielsweise eingesetzt, um ein lokales Netzwerk (LAN) gegen Angriffe aus dem Internet zu schützen.

Firmware
Betriebssoftware für ein Gerät, die üblicherweise in dem Gerät selbst gespeichert ist (ROM).

FTP
„File Transfer Protocol". Das Protokoll und das Programm zum Übertragen von Dateien innerhalb des Internet. Dabei müssen Sie FTP starten, sich mit dem Zielrechner verbinden und einloggen. Auf FTP basiert der Internet-Dienst „Anonymous FTP". Überall auf der Welt gibt es Rechner (FTP-Server)

mit frei zugänglichen Bereichen auf der Festplatte, von denen Sie Informationen aller Art, Public-Domain- und SharewareProgramme für verschiedene Betriebssysteme kostenlos laden können.

Gateway
Schnittstelle zwischen zwei Netzwerken. Ein Gateway-Rechner ist ein spezieller Rechner, der an beide Netze angeschlossen ist und verschiedene nicht kompatible Übertragungsprotokolle übersetzen kann. Im Internet stellen Gateways die Verbindung zwischen dem Internet u. a. Netzwerken her (s. auch „Netzwerkmaske").

Host
englisch, „Gastgeber"
In einem Netzwerk der Hauptcomputer, der das Netzwerk und die angeschlossenen Computer steuert und überwacht, also der Server. In der Datenfernübertragung (DFÜ) der angerufene Computer.

HTTP
„Hypertext Transfer Protocol" - Protokoll für die Übertragung von Informationen im World Wide Web.

H.323
ITU-Standard für Bildtelefonie und Videokonferenzsysteme über LAN- oder Internetverbindungen, um die Kommunikation zwischen Geräten verschiedener Hersteller zu ermöglichen.

ICMP
Das ICMP-Protokoll dient zur Übermittlung von Informationen über das Netzwerk selbst, wie z. B. die Verfügbarkeit bestimmter Pfade innerhalb des Netzwerks, ob bestimmte Rechner erreichbar sind usw. So sendet beispielsweise das für Diagnosezwecke oft eingesetzte „ping" ein ICMP-Paket an den Zielrechner mit der Aufforderung, dieses Paket unverändert zurückzusenden (ICMP echo request).

IP-Adresse (dynamisch/statisch)
IP ist das Internet-Protokoll und gehört als solches zur Protokollfamilie TCP/IP. Das Protokoll sorgt dafür, dass zu übertragende Daten in Paketen zu 64 kBit zusammengefasst werden. Ferner wählt das Protokoll die optimale Route beim Transport eines Datenpakets im Internet aus. Diesen Prozess nennt man Routing.
Damit das IP funktionieren kann, wird jedem Teilnehmer im Internet eine eindeutig identifizierbare IP-Adresse zugeteilt - für den technisch weniger versierten User ist nur das interessant. Diese Adresse umfasst 32 Bit, ist rein numerisch aufgebaut und in vier Gruppen à 8 Bit unterteilt. Jede dieser 8-Bit-Binärzahlen entspricht einer Dezimalzahl zwischen 0 und 255.
Ständig im Netz befindliche Server haben neben der IP-Adresse auch einen Domain-Namen aus Buchstaben, Zahlen und Sonderzeichen, der mnemonischen Gesichtspunkten folgt, sich also leichter merken lässt. Dieser Name wird von speziellen Name-Servern im Netz automatisch in die IP-Adresse übersetzt, damit das IP damit arbeiten kann.
Eine statische IP-Adresse wird fest vergeben (meistens von einem Provider), eine dynamische wird bei jedem Verbindungsaufbau zu einem Server neu vergeben (s. auch DHCP-Server/-Client).

LAN
Abkürzung für englisch Local Area Network, Netzwerk von Computern, das meist auf ein Gebäude beschränkt ist. Es besteht aus PCs und Workstations, die ihre Ressourcen den anderen Computern im Netzwerk zur Verfügung stellen; z. B. können alle an ein LAN angeschlossenen Computer einen zentralen Drucker benutzen. Die Computer können kreis- oder sternförmig angeordnet und über einen Bus miteinander verbunden sein.

MAC-Adresse
(Media Access Control) eindeutige, unveränderbare Hardware-Adresse.

Metrik
Zahlenwert - gibt an wieviele Sprünge innerhalb einer Route benötigt bzw. zulässig sind.

NAT
Network Address Translation (NAT)
Verfahren zur Zuordnung interner und externer IP-Adressen. Mithilfe dieses Verfahrens wird es möglich, dass im Internet ungültige IP-Adressen z. B. aus einem privaten Netzwerk auf im Internet gültige IP-Adressen umgesetzt werden. So kann ein NAT-fähiger Router oder PC ein ganzes Netzwerk hinter einer einzigen IP-Adresse „verstecken".

Netzwerkmaske
Wenn ein Rechner ein Datenpaket an einen anderen Rechner schicken will, muss er zunächst feststellen, ob sich der Zielrechner innerhalb oder außerhalb seines eigenen Netzwerks befindet. Dazu zieht er seine eigene IP-Adresse und die sog. Netzwerkmaske heran und verknüpft diese Angaben miteinander. Pakete in das eigene Netzwerk wird er dann direkt senden, während er Pakete an ein fremdes Netz dem „Default-Gateway" übermittelt. Dieses ist dann dafür verantwortlich, das Paket richtig weiterzuleiten.

NNTP
„Network News Transport Protocol". Protokoll für den Austausch von News-Artikeln zwischen Rechnern im Internet.

NTP
Das NTP „Network Time Protocol" wird genutzt, um Uhren von Computern über ein Netzwerk zu synchronisieren.

Passwort
Zugangsschutz z. B. zum Konfigurationsprogramm, um Änderungen durch unberechtigte Personen zu verhindern.

Peer to Peer-Netzwerk
Kleines Netzwerk zwischen nur wenigen Rechner ohne speziellen Server.

Ping
Packet Internet Grouper, Programm zum Testen der Erreichbarkeit eines Netzwerkservers per IP-Nummer, benutzt das ICMP-Protokoll.

POP
„Post Office Protocol". Protokoll zum Zugriff auf zentrale Mail-Server, die E-Mail für andere Rechner bereithalten - zum Beispiel für Rechner mit SLIP-Verbindung. Es existieren die Versionen POP, POP2 und POP3, die nicht untereinander kompatibel sind.

Port
Ein einziger Rechner kann gleichzeitig mehrere Verbindungen aufbauen und auch mehrere Dienste für andere Rechner zur Verfügung stellen. Zur Unterscheidung dieser parallel laufenden Verbindungen werden die so genannten Ports verwendet, von denen es für TCP und UDP jeweils 65535 gibt. Aufgrund einer allgemeinen Vereinbarung bieten Rechner ihre Dienste üblicherweise auf den Ports 1 .. 1023 an. Abgehende Verbindungen werden normalerweise von Ports ab 1024 aufgebaut. Diese Festlegung ist aber nur eine Konvention und nicht technisch bedingt. Es kann durchaus sinnvoll sein, Dienste auf „hohen" Ports (Ports über 1023) anzubieten. Da traditionell auf den niedrigen Ports auch potentiell unsichere Dienste angeboten werden, sind die meisten Firewalls so konfiguriert, dass auf diese Ports nur sehr eingeschränkt zugegriffen werden darf. Auch sind üblicherweise besondere Rechte (root- bzw. Administrator-Rechte) erforderlich, um Dienste an Ports unter 1024 binden zu dürfen.

Port Forwarding
Anfragen an einen bestimmten Internet-Port werden auf einen Port eines anderen Rechners umgeleitet.

Real Audio
Ein Verfahren zur Echtzeit-Übertragung von Audiodaten über das Internet. Wird unter anderem von „Radiosendern" im Internet benutzt.

RFC
„Request For Comment". Die RFCs beschreiben sämtliche Internet-Protokolle sowie Standards, Verfahren, Algorithmen, Regeln und Strategien der Kommunikations- und Netzwerktechnik. Ein RFC ist nur eine Empfehlung und wird nicht von einem förmlichen Gremium beschlossen. Er ist durch die Veröffentlichung im Internet zur Umsetzung in Hardware und Software freigegeben. Standards, die in RFCs formuliert wurden, haben sich üblicherweise in kürzester Zeit durchgesetzt.

Router, Routing
Router verbinden entfernte Netzwerke miteinander, z. B. das lokale Netz mit dem Internet.
Die PC-Anwendungssoftware „sieht" das Internet durch den Router völlig transparent, ohne dass im Web-Browser hierfür eine spezielle Konfiguration erforderlich wäre.
Router sind je nach Größe und Anwendung meist mit diversen Zusatzfunktionen zum Filtern von Datenpaketen und zum Schutz des lokalen Netzwerkes gegen externe Angriffe ausgestattet.

Service Provider
Bezeichnung für einen Dienstleister, der z. B. einen Zugang zum Internet anbietet.

SMTP
„Simple Mail Transport Protocol“. Internet-Protokoll für den Austausch von E-Mails zwischen Rechnern.

SNTP
Simple Network Time Protokoll - Wird von Uhrzeitervern benutzt und dient zur Synchronisation von Rechnern im Internet.

SSH
Das SSH „Secure Shell“ – Protokoll dient zur Authentifizierung und sicheren, verschlüsselten Datenübertragung.

Subnetzmaske
Die IP-Nummern sind in Kontingente eingeteilt. Es wird zwischen Klasse A-, B- und C-Netzen unterschieden. Zu jeder Klasse gehört eine Subnetzmaske, die die relevanten Bits ausmaskiert: 255.0.0.0 für Klasse A, 255.255.0.0 für Klasse B und 255.255.255.0 für Klasse C. Bei sogenannten angepassten Subnetzmasken sind auch dazwischenliegende Masken möglich, z. B.: 255.255.240.0.

TCP/IP Netzwerkprotokoll
Abkürzung für Transmission Control Protocol/Internet Protocol. Ein Übertragungsprotokoll für Netzwerke, das auch für die Verbindung zum Internet verwendet wird.

Telnet
Name für ein Protokoll und das Programm, das dieses Protokoll nutzt. Sie können damit die Ressourcen von anderen Rechnern online nutzen. Üblicherweise benötigen Sie dafür eine Benutzerkennung auf dem Zielrechner. Doch auch ohne sie können Sie mit Telnet eine Reihe von Aufgaben erfüllen. Viele Rechner bieten per Telnet den Zugriff auf Online Datenbanken an.

T.120
ITU-Standard, der die gemeinsame Nutzung einer Applikation auf verschiedenen Rechnern innerhalb eines Netzwerkes parallel zur Bild- und Tonübertragung ermöglicht

URL
(Uniform Ressource Locator) Eine URL ist eine eindeutige Identifikation einer Ressource (z. B. einer Datei oder Webseite) durch die Zugriffsmechanismen (z. B. HTTP oder FTP) und den Standort (Server). Im Internet bezeichnet die URL die Internetadresse, z. B. http://www.detewe.de. Der wichtigste Teil ist die Domain (im Beispiel „detewe.de“) zusammen mit dem vorangestellten Rechnernamen (hier „www“). Davor kommt durch „://“ abgetrennt das Protokoll (hier: HTTP). Durch Schrägstriche getrennt kann hinten noch ein spezieller Dateiname bzw. Pfad angehängt werden.

VCI
„Virtual Circuit Identifier“ - Zugangsparameter für ADSL-Modems.

Virtueller Server
... benötigt man, um Dienste, die firewallbedingt eigentlich nur im LAN zur Verfügung stehen, auch vom Internet her zugänglich zu machen. Da die Rechner im LAN keine im Internet gültigen IP-Adressen haben, müssen diese Adressen hierfür in die jeweils vom Provider zugeteilte IP-Adressen der WAN-Schnittstelle umgesetzt werden.

VPI
„Virtual Path Identifier" - Zugangsparameter für ADSL-Modems.

WAN
(Wide Area Network) Bezeichnung für ein überregionales Netzwerk, wie z. B. das Internet (vgl. auch LAN - Local Area Network).

Zugangsrechner (Host uniq)
Für den Fall, dass mehrere PPPoE-Verbindungen über eine DSL-Strecke genutzt werden (prinzipiell möglich, aber nicht von jedem Provider unterstützt), müssen die Verbindungen auseinander gehalten werden können. Der Eintrag „Zugangsrechner" kann daher frei gewählt werden.
Wenn keine gegenteilige Information des ISPs vorliegt, sollte dieses Feld leer gelassen werden. Ein Eintrag, der von der Gegenseite nicht akzeptiert wird, führt dazu, dass keine PPPoE Verbindung hergestellt werden kann.

Service und Gewährleistung

Im Problemfall wenden Sie sich bitte an unsere Consumer-Supportline in Berlin,

Tel. 09001 – DeTeWe (=09001 – 33 83 93)
(0,62 € / Minute, aus dem Mobilfunknetz bitte 01901 - 33 83 93 wählen)

Fax 01805 – 33 83 94 (0,12 € / Minute)

Oder Sie benutzen unsere Supportformulare im Internet unter

www.detewe.de

Sollte ein Defekt auftreten, der sich mit Hilfe unseres Supports nicht beheben lässt, schicken Sie bitte das komplette Gerät (mit Netzteil und Anschlusskabel und einer Kopie des Kaufbelegs sowie einer genauen Fehlerbeschreibung) an folgende Adresse:

DeTeWe Deutsche Telephonwerke AG & Co.
Service Center Berlin
Wendenschloßstr. 142,
12557 Berlin

Während einer Dauer von 24 Monaten ab dem Kaufdatum entstehen Ihnen für die Behebung von Gewährleistungsfällen und Rücksendung an Sie keine Kosten.
Falls Sie ohne vorherige Kontaktaufnahme Ihr Gerät zu uns zurückschicken, wird Ihnen im Falle der Fehlerlosigkeit eine Bearbeitungsgebühr in Rechnung gestellt.

Hinweis

Für Kostenvoranschläge für Reparaturfälle außerhalb der Gewährleistung wird eine Bearbeitungsgebühr berechnet, falls es nicht zur Durchführung der Reparatur kommt.

Konformitätserklärung

CE-Zeichen

Dieses Gerät erfüllt die Anforderungen der EU-Richtlinie:
1999/5/EG Richtlinie über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität.
Die Konformität mit der o. a. Richtlinie wird durch das CE-Zeichen auf dem Gerät bestätigt.

Die Konformitätserklärung kann unter folgender Adresse im Internet eingesehen werden:

http://www.detewe.de

Stichwortverzeichnis

A
ADSL....4
Anforderungen an die PCs....7
Anschlüsse....4
Aufstellungsort....2

B
Basiswissen....3
Betriebssoftware....93

C
CAPIControl....96
CE-Zeichen....124

D
Datensicherung....41
Default-Gateway....58
DHCP Server....55
DHCP-Protokoll....71
DNS....59
DNS-Protokoll....70
DNS-Server....58
Domain-Name....58, 59
DoS (Denial of Service)....85
Druckertreiber....90
DSL....32, 50
Dynamisches DNS....35

E
Entsorgung....111

F
Fernwartung....39
Fernzugriff....40
Filesharing....72
Filtern von Paketen....82
Firewall....79
Firmware Update....43
FTP-Protokoll....70

G
Gewährleistung....123
Glossar....116

H
Hacker-Abwehr....84
HomeNet Control....101
HTTP-Protokoll....70

I
ICMP-Protokoll....70
Inhalt der Verpackung....7
Installation....7
Installationsprogramm....93
Internet (Konfigurator)....31
Internetzugang....16
IP-Adresse....53
IP-Adresse, feste....55
IP-Adressen....68
ISDN Fallback....51
ISDN-Fallback (Konfigurator)....33

K
Konfiguration OpenComNet 20....21
Konfiguration PC....11
Konfiguration sichern....41
Konfiguration Telefonanwendung....94
Konfiguration wiederherstellen....42
Konfiguration WinSuite....103
Konfigurator....30
Konformitätserklärung....1, 124
Konten....49

L
LAN....52
Leasetime....57

Leuchtdioden 5
Lieferumfang 7
Logbuch 89

M
Montage 9
MTU 58

N
NAT 67
Netzwerkdrucker 90
Netzwerkklasse 54
Neustart 44

O
Online Spiele 73

P
Passwort 38
Pflege und Wartung 111
Port Forwarding 67
Ports 71
Protokolle 70

R
Rechnernamen 59
Relay 59
Routen 64

S
Server 59
Service 123
Sicherheit 76
Sicherheitshinweise 1
Sicherheitsoptionen 78
SMTP/POP3/IMAP-Protokolle 70
SNMP-Protokoll 71
SNTP 47
SNTP-Protokoll 71
Software installieren 93
Software-Ausstattung 6
Spezielle Anwendungen 74
Spoofing-Angriffe 85
Status 88
Stromversorgung 1
System (Konfigurator) 37
System-Info 87

T
TCP-Protokoll 70
TCP/IP Einstellung unter Windows XP 14
TCP/IP Einstellungen - Übersicht 11
TCP/IP Einstellungen unter Windows 2000 .13
TCP/IP Einstellungen unter Windows 98 SE 12
Technische Daten 110
TFTP-Protokoll 71
Tischaufstellung 10
TTL 58

U
Überblick 3
UDP-Protokoll 70
Uhr 45
Umgang mit dem OpenComNet 20 1
Umwelteigenschaften 111
UPnP (Universal Plug and Play) 86

V
Verpackungsinhalt 7
Victim Protection 85
Virtueller Server 67
Voice over IP (VoIP) 71
Voraussetzungen für den Betrieb 7

W
Wandmontage 10
Werkseinstellungen 22
Wins-Server 58
WinSuite 93, 103

Z
Zugangskontrolle 80

Notizen

Bohrschablone

DeTeWe AG & Co. KG · Zeughofstraße 1 · 10997 Berlin • www.detewe.de

Mat.-Nr. 69960.029
Stand 01/05
Technische Änderungen vorbehalten